CHRISTIAN SERVICE UNIVERSITY COLLEGE

DEPARTMENT OF COMPUTER SCIENCE

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

NETWORK MONITORING, MANAGEMENT AND SECURITY SOFTWARE
(KAK-BONSU NETWORK WATCHER)

A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A DEGREE IN BACHELOR OF SCIENCE IN COMPUTER SCIENCE

BY

KAKRABA GEORGE

TEDDY OSEI BONSU

JUNE, 2014

STATEMENT OF AUTHENTICITY

We have read the university regulations relating to plagiarism and certify that this report is all our own work and do not contain any unacknowledged work from any other source. We also declare that we have been under supervision for this report herein submitted.

GEORGE KAKRABA 10140955…………………… ………………………
(Student) **Signature** **Date**

TEDDY OSEI BONSU 10149281…………………… ………………………....
(Student) **Signature** **Date**

SUPERVISOR'S DECLARATION

We hereby declare that the preparation and presentation of the dissertation were supervised in accordance with the guidelines on supervision laid down by Christian Service University College.

Certified by
Mr.Christopher Ayaaba Abilimi ……………………… …………………………
(Supervisor) **Signature** **Date**

Dr. Thomas Yeboah ………………………. ………………………...
(Head of Department) **Signature** **Date**

ABSTRACT

Network monitoring, management and security software are created to collect data for network monitoring, management and security applications. The purpose of network monitoring, management and security software is the collection of useful information from various parts of the network so that the network can be managed and controlled using the collected information. Most of the network devices are located in remote locations. These devices do not usually have directly connected terminals so that network management application cannot monitor their statuses easily. Thus, network monitoring, management and security software are developed to allow network administrators or system administrators to check the states of their network devices.

DEDICATION

This project work is gratefully dedicated to the Almighty God for seeing us through this course and especially to our family, friends, and our loved ones. We also dedicate this work to our project supervisor, Mr. Christopher Ayaaba Abilimi for his time, guidance, attention, corrections and suggestions.

ACKNOWLEDGEMENT

We would like to express our deepest appreciation to all those who provided us with the possibility to complete this project. A special gratitude we give to our final year project Supervisor, Mr. Christopher Ayaaba Abilimi, whose contribution in stimulating suggestions and encouragement, helped us to coordinate this project.

Furthermore, we would also like to acknowledge with much appreciation the crucial role of the head of Department, who gave the permission to use all required equipment and the necessary materials to complete the task "Dr.ThomasYeboah". Last but not least, many thanks go to the head of the project Mr. Christopher Ayaaba Abilimi who have invested his full effort in guiding the team in achieving the goal.To the head of department and lecturers of computer science department (Christian Service University College, Kumasi) for their patience and support during our period of study.

TABLE OF CONTENT

CHAPTER ONE

INTRODUCTION

CHAPTER TWO

LITERATURE REVIEW

CHAPTER THREE

METHODOLOGY

CHAPTER FOUR

TESTING OF THE SOFTWARE

CHAPTER FIVE

CHAPTER SIX

DOCUMENTATION

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The need to be able to manage network resource monitoring and be able to track all transmission has been a great worry for some organizations. To effectively be able to have a total control there must be software that should be able to track online usage of resources.

The effective usage of monitoring software is that, it needs to monitor the network continuously without it being left for even a second, since it cannot be determine when an error or attack will happen, this makes it time consuming and the need to employ someone solely for the monitoring, in view of that the network monitoring, management and security software will have an alert feature that will prompts users by SMS or email within the shortest time to alert the administrator or the user(RD Austin, CAR Darby - The myth of secure computing ,Harvard Business Review, 2003).

Being able to identify individual users working on various workstations and their activities that they are performing on the workstation as part of internal monitoring problems .The monitoring software will have a feature that will allow remote desktop viewing while the users still work un interacted and their desktop can be locked if any malpractice is detected .this remote feature will go beyond the normal windows remote desktop feature that allow only one person to logon to the system at a time and it will block the current user using the system unless the remote user finishes to use the system .This software will allow more than one person to logon to the remote workstation and still allow users to have access to their stations (Schneir, B. (2005), Managed Security Monitoring: Network Security for the 21st Century).

Performance of network resource monitoring which will allow the user to be able to know the performance level of hard drive , processor ,memory and network load which will help administrators to have control on their network .In view of this our software will have the feature that will be able to determine the work load of the system and give accurate results on the use of the resources of the system and trigger alert if the resource is been over utilized and it reaches it peak level the measurement will be in using the clock rate of the processor or memory depending on which of the resource is being monitored.

The software will be able to check the normal working load of all workstations and if there is any problem such as low current to devices, unauthorized use of a system password, duplication logon with same id to different system etc it will log the report and prompt the system admin of the incident.

Identifying workstations that belong to a network by a system administrator is one of the biggest challenges since it is difficult to even monitor names with large networks .The software will record mac-addresses of workstations that will be connected and it will be connected to already document mac-address softcopy of the system. If the mac-address does not match it will filter the workstation out and disconnect the workstation (Rasmussen, S. (2002). Centralized Network Security Management, Combining Defense in Depth with Manageable Security, SANS Institute Security Reading Room, Retrieved May, 2014, from http://www.sans.org/ reading room/).

Network messaging allows information to be sent to network users desktop instantly to alert them of emergencies or in prompt meeting times or even to stop them from performing certain unauthorized activities. Our software will be able to send messages to all users desktop and even alert them through their emails or phones.

The network monitoring, management and security software, combines an easy-to-use interface that lets you quickly deploy the product for production and also apply your organization's monitoring policies across multiple devices quickly.

The software will provide basic functionality across critical IT resources such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, virtual servers, domain controllers & other IT infrastructure devices.

The software will be used to track all machines connected to the network with their MAC Address, machine names and status of connection to the network etc. It will also be used to administer the network in terms of printer installations, creating secured users using VB Scripts. It will also have a secure VPN feature to be able to scan the internet for available machine that have connected the network. The project will be based on using server 2008 to create a domain controller and be able to design scripts to perform certain functions the operating system cannot perform like creating policies for clients that logon to the network as a way of controlling user desktop and environment functionality .Whiles all transmission will be monitored from source to destination .Network attacks like MAN IN THE MIDDLE, BRUTE FORCE ATTACK ETC will be search for by the software .It is essential for an Administrator to be able to have total control of machines and all transmission so the software will create a network topology for online machine and all websites viewed will be displayed by the software (RH Dev, MH Nelson, Method and apparatus for monitoring the status of non-pollable device in a computer network).

The software we are designing is to be able to monitor live events on the network and also to monitor any new connections to the network .some features like DNS intrusion detection, IP spoofing etc will be added .The software will be able to record the IP addresses, MAC addresses, model of machines, authenticated user on the machine, shutdown the systems remotely.

1.2 OBJECTIVE OF THE STUDY

The main objective of the project is to design and develop a network monitoring, management and security software for organizations which will present a framework for security administrators and security personnel to monitor their complex network devices more easily, and a means to present the results of their work in an easy-to-understand fashion to their superiors and to top management.

1.2.1 Specific Objectives:

1. To determine the type of networks used by organizations
2. To determine how network, monitoring, management and security software will enhance the operations of the work environment
3. To minimize the challenges/problems associated with the current monitoring software
4. To know the benefits of network monitoring, management and security software to organizations.

1.3 RESEARCH PROBLEM STATEMENT

With the study of network monitoring, management and security, it was observed that system administrators hardly find out about an intrusion which often means they only find out about critical problems when users complain. It was also observed that it takes a lot of time to solve issues. On average, it takes five hours from the moment a critical problem occurs to detecting it, determining the problem's cause and correcting," an excerpt from the study explained (Nathan Eddy, Associate Editor, www.eweek.com,accessed on 14/01/2014).

It was observed that Network monitoring, management and security issues are of little use without accurate, up-to-date reports that allow network managers to make correct decisions. Unfortunately, fault reporting seems to be one of the field's weakest areas. According to Guy Antony Halse, Novel Approaches to the Monitoring of Computer Networks, 2003, traditionally, fault reports are limited to the symptomatic reporting of the problem, with the network manager being left to interpret these symptoms — much like a doctor diagnoses ailments from a list of symptoms. This method works very well in a large number of cases, but breaks down in loosely structured organizations where the realm of responsibility is not delegated to one body. For example, being told that the departmental mail server has stopped working is not particularly useful if the underlying ailment is a faulty DNS server managed by a different organizational division. In cases like these, network monitoring, management and security software should be able differentiate between faults that are within the divisional realm of responsibility, and those that fall beyond it. This is something that symptomatic reporting does not cater for very well (Guy Antony Halse, Novel Approaches to the Monitoring of Computer Networks, 2003).

Further complicating matters, Guy Antony Halse, Novel Approaches to the Monitoring of Computer Networks, 2003 stated that the presence of legacy network performance management tools that cannot keep pace with emerging technologies and trends such as cloud computing, enterprise mobility, virtualization, and bring your own device (BYOD) initiatives, which are creating new challenges for IT departments and bringing additional strain to overburdened networks.

It was further noticed that real time operations on the network were not monitored. As resources and other utilities are used by various users without knowing the details of what they are using or what information they require. This leads to unauthorized usage of resources. And to combat the unauthorized usage of resources, network monitoring, management and security software will be used to secure and protect the resources.

1.4 RESEARCH QUESTIONS

The Project is intended to answer the following research questions:

1. What type of network is the organization using or implementing?
2. How can network monitoring, management and security software enhance operations of the work environment?
3. How can network security challenges be minimized by network monitoring, management and security software
4. What are the benefits of network monitoring, management and security software to organizations

1.5 JUSTIFICATION OF THE STUDY

The world is becoming more interconnected with the advent of the Internet and new networking technology. Network monitoring, management and security software is becoming of great importance because of intellectual property that can be easily acquired through the internet. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as “Trojan horses,” planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why network monitoring, management and security software is emphasized in data networks, such as the internet, and other networks that link to the internet.

Deciding specifically what to monitor on your network is as important as giving network monitoring, management and security software a general thumbs up. You must be sure that your corporate network topology map is up to date. That map should accurately lay out the different types of networks to be monitored, which servers are running which applications on which operating system, how many desktops need to be counted into the mix and what kind of remote devices have access for each network. A dose of clarity at the outset makes choosing which monitoring, management and security tools to purchase down the line somewhat simpler.

Network monitoring, management and security can be achieved using various software or a combination of plug-and-play hardware and software appliance solutions. Virtually any kind of network can be monitored. It doesn't matter whether it's wireless or wired, a corporate LAN, VPN or service provider WAN. You can monitor devices on different operating systems with a multitude of functions, ranging from BlackBerrys and cell phones, to servers, routers and switches. The network monitoring, management and security software can help you identify specific activities and performance metrics, producing results that enable a business to address various and sundry needs, including meeting compliance requirements, stomping out internal security threats and providing more operational visibility.

With network monitoring, management and security software, the communication channel will not be vulnerable to attacks as some times possible hackers could try to attack the communication channel, obtain the data, decrypt it and re-insert a false message but will prove furtile due to the operation of the network monitoring ,management and security software.

Network monitoring, management and security software will monitor an internal network for problems. It can find and help resolve snail-paced webpage downloads, lost-in-space e-mail, questionable user activity and file delivery caused by overloaded, crashed servers, dicey network connections or other devices.

Network monitoring, management and security software is quite different from intrusion detection systems (IDSs) or intrusion prevention systems (IPSs). These other systems detect break-ins and prevent scurrilous activity from unauthorized users. With network monitoring, management and security software, it will let you know how well the network is running during the course of ordinary operations, preventing unauthorized users from communicating to and fro from a particular network. It will enhance the confidentiality of information and will also provide authentication that is ensuring that users of the network are who they say they are.

1.6 SIGNIFICANCE OF THE STUDY

The project is aimed at enhancing the accountability of individuals across the network of heterogeneous systems. When a user initially signs onto the network, that user is assigned a network identifier (NID).As the user moves across the network, all activity performed by that user on the host server is mapped to the NID.

The Project will also enhance operations to be monitored without any constraints. It will also facilitate the use of resources.

System Features:

Advantages of the proposed software are listed below:

- **Identification:** The proposed software will enhance the identification of individuals on the network and thus prevent unauthorized usage of the network.
- **Accountability**: The project will also enhance accountability since the administrator will know the particular activities performed by individual on the network.
- **Flexibility**: The easy-to-use network monitoring Performance Monitor provides the comprehensive insight and customizability you need to rapidly find and assess the impact of issues, isolate the cause, and restore performance levels.
- **Real time:** Proactively ensure continuous up-time with alerts and automatic repair of potential problems before users are affected.
- **Managemen**t **Information:** They will be used to provide useful information of management for control and decision making.

1.7 LIMITATIONS

During the study, some aspects were beyond the reach of the researcher. The aspects are number of challenges that were met and these are:

The number of people who are willing to answer the survey. Most system administrators were not willing to answer the survey and are afraid of giving information because of policies regarding their operations of work. Time constraints was also a factor, the time it will take the respondents to answer the survey and analyze the results .Another factor is Financial constrains with which this study was conducted and access to certain information and data were limited.

1.8 DELIMITATION

This research is on network monitoring, management and security and this does not cover areas in monitoring like: Malicious agent or malicious entity security, Data security and Anti-virus software.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

The amount of digital information in the world is increasing, and this digital information is being shared throughout the world. A published Gartner report (Hallawell, 2004) estimated that the volume of information that organizations deal with, will be 30 times bigger in less than a decade. The effects of information systems on daily life began to become significant in the early 90's by the introduction of one of the most exceptional inventions of the century: the Internet. As the days went by many forms of networking have been developed. The motivation behind each new form of networking was basically either to make it possible for monitoring, management and security aspect. One of them is the use of internet. Although the basic applications and guidelines that make the internet possible had existed for almost two decades, the network did not gain a public face until the 1990s. On 6 August 1991, CERN, a pan European organization for particle research, publicized the new World Wide Web project. Minimarts Marketing Group, 2009). There are different means of gaining access to the internet. Some of them are wireless, dial-up and broadband (ADSL). Each of them has its own pros and cons. Based on the pros and cons of the different means of networking, it has become necessary to establish a network monitoring, management and security software. Network monitoring, management and security software can benefit an organization in many ways. It helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Daily log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred.

Network monitoring, management and Security is responsible for securing the network, the management system that manages the networks and management transactions. In addition, it is intended to prevent intrusion if at all possible, to detect intruders in case of intrusions promptly and to recover from and limit the consequences of such intrusions as efficiently as possible. Here, the manager is informed of who is using the network. (Haojin 1999, 433.) All of these functional divisions are what make up the monitoring and controlling parts of the network management. When considering network monitoring, management and security, performance is very important.

However, according to the predictions of many security specialists, threats cannot all be eliminated; furthermore, the growth rate of security threats will be bigger than the growth of the Internet (Schneir, 2005). This emphasizes the necessity of network monitoring, management and security software in workstations.

2.2 THEORITICAL FRAMEWORK

Software is a general term. It can refer to all computer instructions in general, or to any specific set of computer instructions. It is inclusive of both machine instructions (the binary code that the processor "understands") and source code (more human-understandable instructions that must be rendered into machine code by compilers or interpreters before being executed).

Software is a set of programs, procedures, functions, associated data and/or its documentation, if any. Program software performs the function of the program it implements, either by directly providing instructions to the digital electronics or by serving as an input to another piece of software. Software is also sometimes used in a more narrow sense, meaning application software only. (wikipedia.org/wiki/Software accessed on 01/11/13)

2.3 SOFWARE APPLICATION DOMAINS

Monitoring entails a system that constantly observes and analyzes the status and behavior of network which comprises network devices such as switches, hubs, routers, printers, computers and their associated services.

At the most basic level, network monitoring is done by sending a ping, which is a monitoring tool that requires instantaneous reply from each computer or network device on the network. If such a network device fails to respond or takes too long to respond, the network monitoring system notifies the network administrator of the problem. (Dev, Emery, Rustici, Brown, Wiggin, Gray & Scott, 1996.)

However, network monitoring domain handles the monitoring of the network by continuously taking regular virtual snapshots of the network's workflow. Also track records of irregularities discovered in the workflow are kept. In the event whereby such irregularities are so deviated from the recorded snapshots, the network administrator will be notified. (Afeez Yusuff, Network monitoring, Bachelor's thesis Central Ostrobothnia university of applied Sciences Degree Programme in Information Technology ,May 2012a**)**

Management

Network management (NM) refers to the broad subject of managing computer networks. NM consists of a set of functions to control, plan, deploy, allocate, coordinate, and manage network resources. It involves a number of software and hardware products that system administrators use to manage a network. (Webopedia, 2013)

Network Management can be identified as any approach that includes monitoring the performance of the network, detecting and recovering from faults, configuring the network resources, maintaining accounting information for cost and billing purposes, and providing However, network management covers a wide area, including performance, fault, and configuration. These aspects will be detailed later in this work. In general, network management functions include verification of the status of all network devices such as routers, switches, hubs and computers. NM also entails recording and analyzing error messages from all the aforementioned devices in order to monitor the health of all devices (Sebastian & Adrian 2009, 79.)

Security Domain is responsible for securing the network, security domain is intended to prevent intrusion if at all possible, to detect intruders in case of intrusions promptly and to recover from and limit the consequences of such intrusions as efficiently as possible. Here, the manager is informed of who is using the network. (Afeez Yusuff, Network monitoring, Bachelor’s thesis Central Ostrobothnia university of applied Sciences Degree Programme in Information Technology ,May 2012b**)**

CHAPTER THREE

METHODOLOGY

3.1 INTRODUCTION:

This chapter outlines the techniques, procedures and processes used in the gathering and analysis of the needed requirements in the development of Network monitoring, management and security software. It explains how the software is supposed to function in order to meet the stakeholder's requirements. The research design, approach and strategy are treated in this section. The software development life cycle used in carrying out the project is the Waterfall model**.**

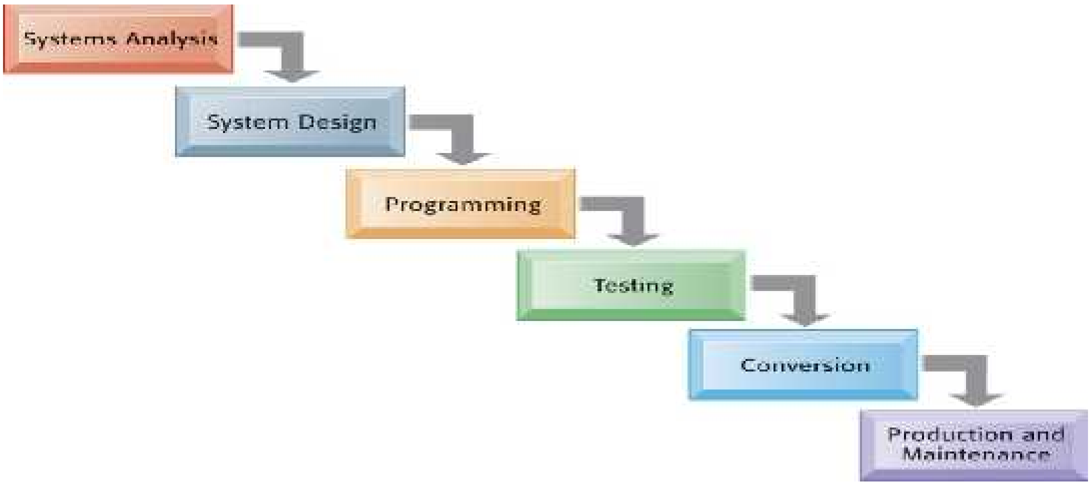


***Figure* 1:** Depicting waterfall development model

This chapter also introduces general concepts, mechanisms, and systems for monitoring, management and security distributed environments. Developing and maintaining complex applications has become impossible without a sufficient tool support. Monitoring, management and security software provide the basis for on-line tools, which are a major technique for handling the on-line phases of the software lifecycle.

3.2 RESEARCH DESIGN

The research design attempts to provide the best information possible subject to the variant constraints which the research was conducted in other to answer the research objectives. The research employed the descriptive and analytical method which seek to describe the phenomena, gives a clear picture of trends, an event or situation. The study employed the descriptive survey method in looking at network monitoring, management and security software.

3.3 RESEARCH APPROACH

Basically, tools are programs used to support or simplify the development and deployment of applications. This comprises software development tools like integrated development environments with analysis and design tools, GUI builders, and debuggers, as well as on-line tools that are applied to the developed application at runtime. In contrast to off-line tools that only collect information at runtime for later analysis, the characteristic of on-line tools is to allow immediate manipulations of the running program in addition to data collection. (Günther Rackl, Monitoring and Managing Heterogeneous Middleware)

3.4 RESEARCH STRATEGY

Nick Feamster, Research Statement elaborated that users of computer networks demand high availability and good performance in the face of continually changing network conditions. Most communications networks are kept afloat by the vigilance of network operators, who tune network configurations in response to changes in available resources, failures of network elements, fluctuations in traffic demands, or the onset of malicious or otherwise unwanted traffic (e.g., spam).

Responsiveness to changing network conditions requires increasingly sophisticated detection and mitigation strategies as networks become saddled with more features and subject to new classes of unforeseen threats, and as users demands from the network become increasingly stringent. Network monitoring, management and security software has long been a critical piece of this puzzle: mitigating network disruptions depends, first and foremost, on tools and techniques to quickly and accurately detect these disruptions and determine their causes.

3.5 DATA COLLECTION METHOD

Data collection techniques employed in this study were direct observation and unstructured interviews. The interviews and the observation were guided by the primary research question: “what type of network is the organization using or implementing, how can network monitoring, management and security software enhance operations of the work environment, and how can software security challenges be minimized by network monitoring, management and security software. These methods were used to elicit information from system administrators on their perception on how their networks information or logs are recorded, processed, stored. They also shared their views on the current system being used.

3.6 EVENTS AND ACTIONS

All monitoring techniques rely on the detection of events that are relevant for the program behaviour. Of course, the notion of relevance depends on the specific tool and application; therefore, monitoring systems allow tools to define relevant events dynamically. With these events, certain actions are triggered, i.e. commands that are executed when the event occurs. These commands can either carry out data collection, or also manipulate the running program. The mechanism of events and actions is also called the even-action paradigm. (Günther Rackl, Monitoring and Managing Heterogeneous Middleware).

Network Monitoring, management and security software is a host and is designed to inform you of network problems before your clients, end-users or managers do. It has been designed to run under the Microsoft Windows operating system (ie. Either windows Xp or latest windows versions), Linux. The software runs intermittent checks on hosts and services you specify using external "plugins" which return status information to the software. When problems are encountered, the software can send notifications out to administrative contacts in a variety of different ways (email, instant message, SMS, etc.).

3.6.1 Observation

This technique was used when the validity of data collected through other methods is in question or when the complexity of certain aspects of the data system prevents a clear explanation by the end users. Data gathered through observation are very reliable and relatively inexpensive compared to other fact finding techniques. Observation, a fact-finding technique, involves the researcher becoming an observer of people and activities in order to learn about the system.

3.6.2 Interview

The personal unstructured interviews which involve asking open-ended questions were recognized as the most important and most often used fact-finding technique to get the system administrators involved in identifying requirements, and solicit ideas and opinions. The interviews placed emphasis on network administrators, the most important elements of information gathering, to respond freely and openly to questions. By establishing rapport, the researcher was able to give the interviewees a feeling of actively contributing to the software development and probe for more feedback from the interviewees.

3.7 SYSTEM REQUIREMENT

Computer software requires certain hardware components, known as system requirement, to be present in order to function effectively. Verification of the finished product to ascertain if requirements have been met ensures that the software works efficiently with respect to time, money and other resource include:

The Server

- A minimum of windows server 2003 operating system.
- Pentium IV one Gigahertz and above.
- Keyboard and mouse.
- Hard disk of 200 gigabyte and above.
- Memory of 3 gigabyte and up

3.7.1 Justification of Tools:

Why Visual Basic 2010?

- It allows VB developers to do things that we couldn't do before, things like inheritance and structured error handling. Another long-awaited capability is the ability to write applications that interact with the user via the command line. VB.NET makes this easy and with full .NET functionality.
- Visual Basic.Net is totally object oriented
- Visual Basic.Net provides managed code execution that runs under the Common Language Runtime (CLR), resulting in robust, stable and secure applications. All features of the .NET framework are readily available in VB.NET.

- Security has become more robust in VB.NET. In addition to the role-based security in VB6, VB.NET comes with a new security model, Code Access security. This security controls on what the code can access. For example you can set the security to a component such that the component cannot access the database. This type of security is important because it allows building components that can be trusted to various degrees.

MS SQL Server:

- SQL Server 2008 has reduced application downtime, increased scalability and Performance, and tight yet flexible security controls.
- SQL Server 2008 makes it simpler and easier to deploy, manage, and optimize enterprise data and analytical applications. It enables one to monitor, manage and tune all of the databases in the effective way.
- SQL Server 2008 provides a new capability for the partitioning of tables across file groups in a database.
- SQL Server 2008 has unlimited database as compared to Microsoft Access database which all data across will be conveniently saved.

3.6.2 Functional Requirement

This software requires an I.T. expert to be able to manage and interpret the results that will be generated by the monitoring software. The user who will manage this software should have network administration background.

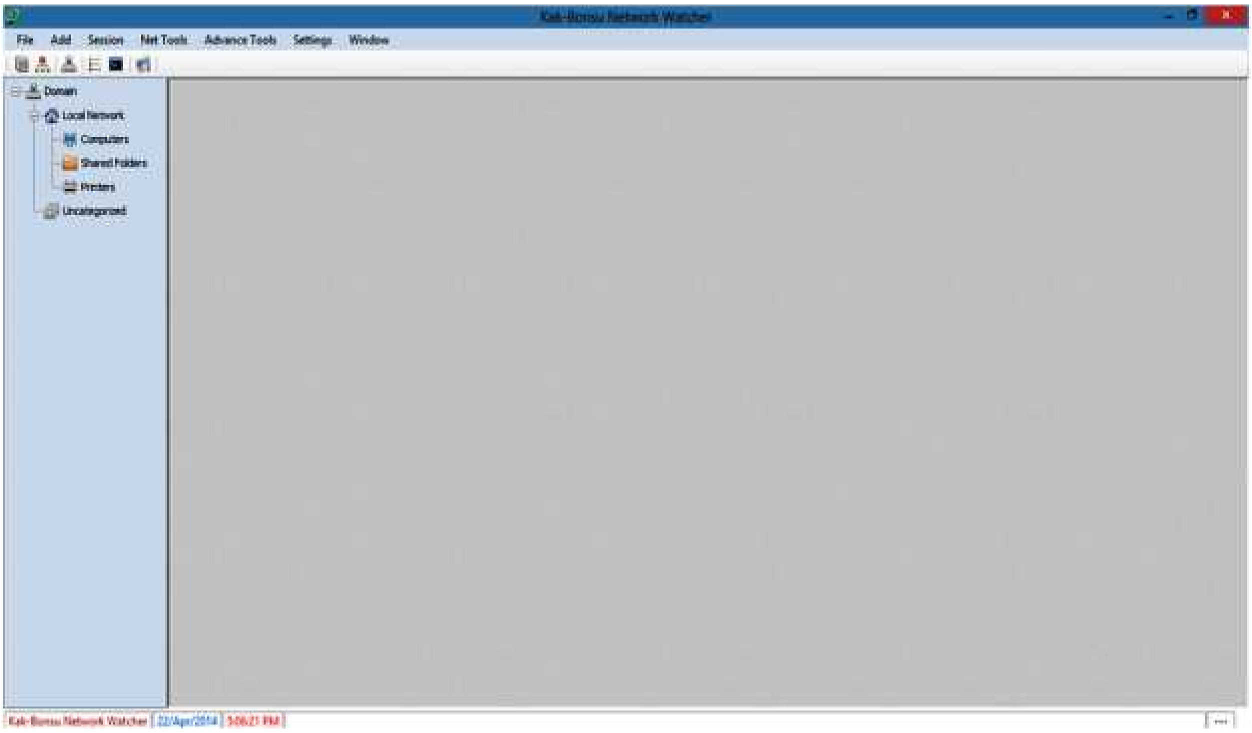
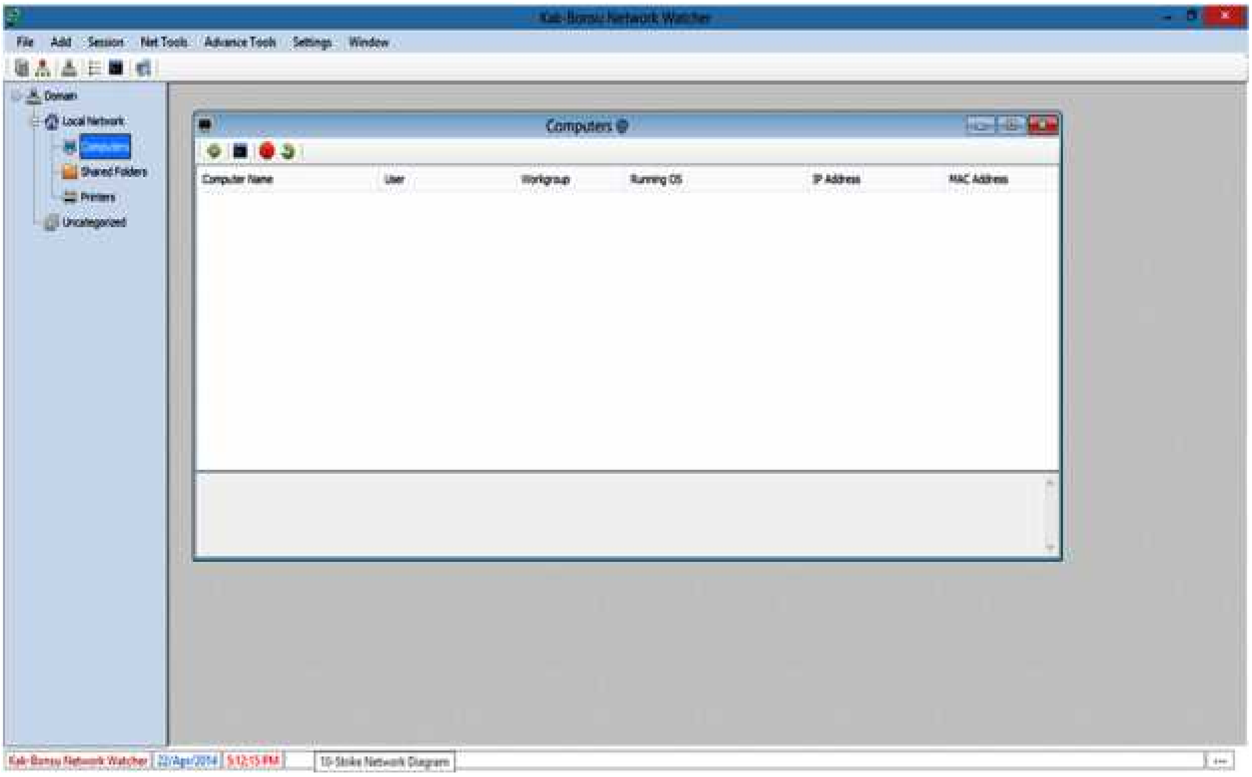
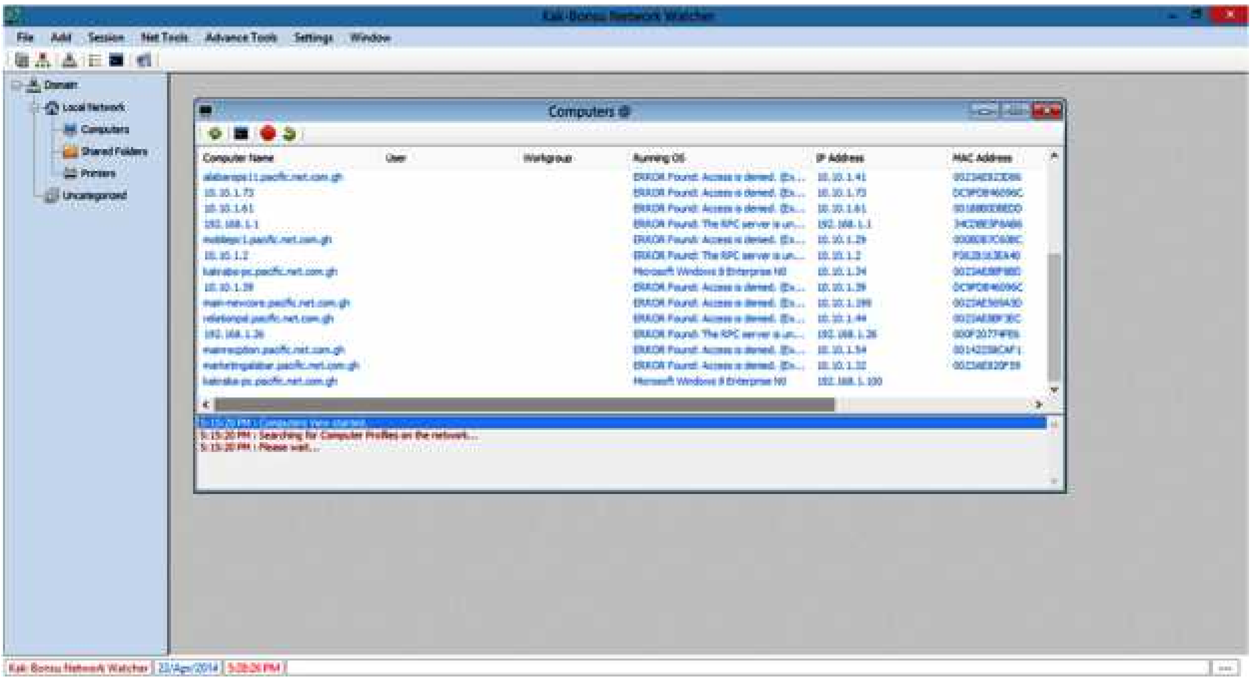


Figure 2**:** Software and its functionalities



Computer Name	User	Workgroup	Running OS	IP Address	MAC Address

Figure 3: Network and its protocol functionalities

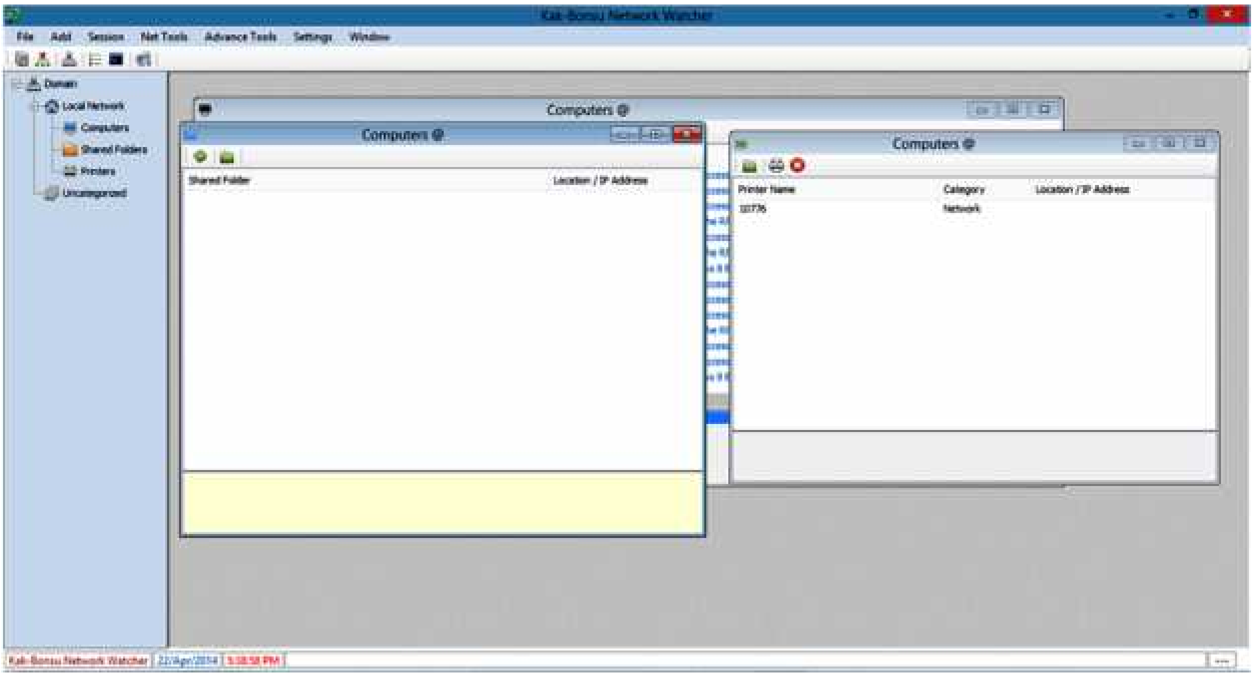


Computer Name	User	Workgroup	Running OS	IP Address	MAC Address
alabaropc11.pacific.net.com.gh			ERROR Found: Access is denied. (Ex...	10.10.1.41	0023AE0323D86
10.10.1.73			ERROR Found: Access is denied. (Ex...	10.10.1.73	DC9FDB46096C
10.10.1.61			ERROR Found: Access is denied. (Ex...	10.10.1.61	0018880088ED0
192.168.1.1			ERROR Found: The RPC server is un...	192.168.1.1	34C0BE3F6A86
mobilepc1.pacific.net.com.gh			ERROR Found: Access is denied. (Ex...	10.10.1.29	000BDB7C60BC
10.10.1.2			ERROR Found: The RPC server is un...	10.10.1.2	F0B2B1E3EA40
kakraba-pc.pacific.net.com.gh			Microsoft Windows 8 Enterprise N0	10.10.1.34	0023AE0BF880
10.10.1.39			ERROR Found: Access is denied. (Ex...	10.10.1.39	DC9FDB46096C
main-newcore.pacific.net.com.gh			ERROR Found: Access is denied. (Ex...	10.10.1.199	0023AE5654D0
relationpst.pacific.net.com.gh			ERROR Found: Access is denied. (Ex...	10.10.1.44	0023AE0BF3EC
192.168.1.26			ERROR Found: The RPC server is un...	192.168.1.26	000F2077 4FE6
mainreception.pacific.net.com.gh			ERROR Found: Access is denied. (Ex...	10.10.1.54	00142258CAF1
marketingalabar.pacific.net.com.gh			ERROR Found: Access is denied. (Ex...	10.10.1.32	0023AE820F59
kakraba-pc.pacific.net.com.gh			Microsoft Windows 8 Enterprise N0	192.168.1.100	

```
5:15:20 PM : Computers View started.
5:15:20 PM : Searching for Computer Profiles on the network...
5:15:20 PM : Please wait...
```

Kak-Bonsu Network Watcher | 22/Apr/2014 | 5:28:26 PM

Figure 4: Depicts captured machines on the network.



Shared Folder	Location / IP Address

Printer Name	Category	Location / IP Address
10776	Network	

Kak-Bonsu Network Watcher | 22/Apr/2014 | 5:38:58 PM

Figure 5: Represent detection of shared Resources

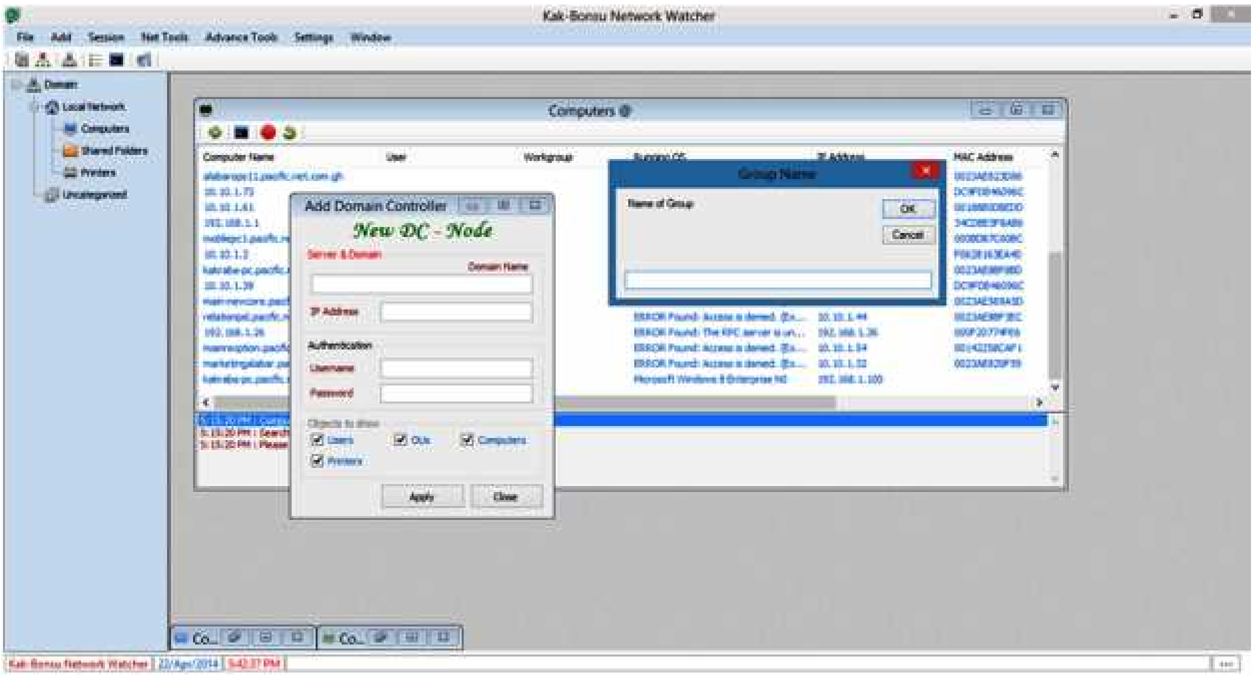


Figure 6: Shows how to manually add a computer to the network

CHAPTER FOUR

TESTING

4.1 INTRODUCTION

This chapter is concerned with the testing of the software. Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include, but are not limited to the process of executing a program or application with the intent of finding software bugs (errors or other defects).Software testing can be stated as the process of validating and verifying that a computer program/application/product:

- meets the requirements that guided its design and development,
- works as expected,
- can be implemented with the same characteristics,
- And satisfies the needs of stakeholders.

Software testing, depending on the testing method employed, can be implemented at any time in the software development process. (Accessed at http://en.wikipedia.org, May 28 2014)

Testing of the software was conducted in two phases-the alpha and beta testing. The Alpha testing is a type of acceptance testing; performed to identify all possible issues/bugs before releasing the product to everyday users or public. The aim is to carry out the tasks that a typical user might perform. Alpha testing is carried out in a lab environment and usually the testers are internal employees of the organization.

To put it as simple as possible, this kind of testing is called alpha only because it is done early on, near the end of the development of the software, and before beta testing.(Accessed on http://www.guru99.com/alpha-beta-testing-demystified.html,may 28 2014)

The Beta test is the process of testing the product amongst system Administrators or Network administrators to confirm that the product works. The beta test consisted of real-time testing in a working environment. This was done by implementing and testing the software on the networks of Pacific Savings and Loans, Reggio Company Limited, Kessben FM and an education institution of computer Training (IPMC). Beta testing involves personal unstructured interviews which involve asking open-ended questions and also soliciting ideas and opinions from network administrators or system administrators. Information gathered from network experts was instrumental in designing the software.

4.2 REQUIREMENT ANALYSIS

Requirement analysis involves personal unstructured interviews which involve asking open-ended questions and also soliciting ideas and opinions from network administrators or system administrators. Information gathered from network experts was instrumental in designing the software.

4.3 DESIGN

Network monitoring, management and security (Kak-Bonsu network watcher) is custom made software based on the preferences of the administrators or network experts interviewed.

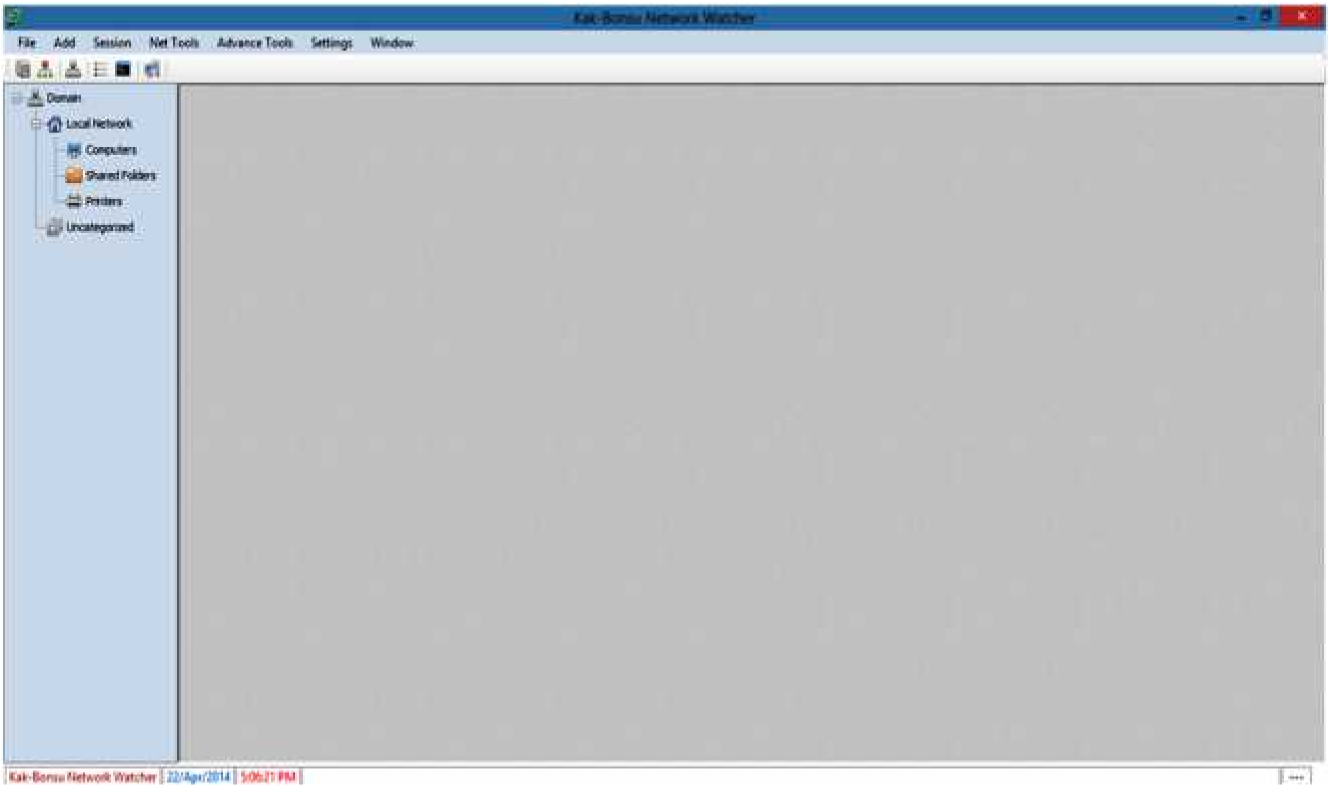


Figure 7: Displays sections of the main page

4.4 IMPLEMENTATION OF THE SOFTWARE

The software was implemented and tested for errors interoperability in an organization. After the testing, it was observed that the software was able to capture details of all the systems connected on the network, such details are the Computer names of the domain they are connected to, Mac address and mode of determining how machines obtain IP address (ie.DHCP or static IP) and the identification of the particular systems as well the operating system a particular system is using. It was again observed that the software can actually capture user activities on the network as well as remotely shutdown a user system. It also sends an alert message to the administrator when there’s a breach of network or an unauthorized usage of the network.

CHAPTER FIVE

EVALUATION OF THE SOFTWARE

5.1 INTRODUCTION

Before considering the outcomes of our research effort, the objective and relevance of this study are revisited for a moment. To determine whether the objective of this study is scientifically sound, we asked ourselves why it was necessary to design a security framework, rather than, for example, design new countermeasures for the malicious host problem. The necessity for a framework can best be described by using an analogy to that of the processes involved in the building of a factory (industrial unit). A structure is needed to establish the outlines and requirements of the design, as well as to provide specifications of how and where the building blocks have to be placed. Without such a structure (in our case the framework), the building blocks (in our case the countermeasures) will be unorganized modules lying in disarray. (Elmarie Biermann, A Framework for the protection of mobile agents against malicious Hosts**,** University of South Africa, September, 2004).

The results obtained from the testing and implementation revealed that the software provide protection for network resources, including against man in the middle attacks and unauthorized usage of resources.

The evaluation of our work considers the two topics general approach, strengths and weakness of the software. Important criteria for our considerations are the software application domains as stated and explained in chapter two.

5.2 STRENGTHS AND WEAKNESS

One of the most fundamental and critical capabilities in the software is establishing accountability for actions performed by individuals. A combination of authentication and auditing mechanisms residing in the software usually provides this accountability. In such systems, the user identifies and verifies him to the authentication mechanism keeps account of the activities performed by that authenticated user.

Unfortunately the accountability can be lost when the user crosses operating system (eg. logging into another host across the network).Although the user will be reauthenticated by the new machine (either with a new password or by trusting the authentication of the first host), the accounting of the users activities will be distributed across the audit trails of multiple hosts. If users are restricted from changing their identification as they move across systems and if the audit timing can be synchronized across auditing mechanisms, accountability can be achieved; however, such restrictiveness is not attainable in many environments.

CHAPTER SIX

DOCUMENTATION

6.1 INTRODUCTION

According to the studies we have done, we define documentation as any artifact that helps communicate information about the software systems and it is expected to provide precise information about software system. (Golara Garousi, a Hybrid Methodology for Analyzing Software Documentation Quality and Usage, September 2012a)

Generally documentation artifacts respond to two main needs:

- it helps a software development team to communicate information about the software system and its implementation details to the maintenance team
- It aims to support software development team members to continuously formulate the solution to be implemented.

Usually documentation arises from the need to manage software projects' knowledge. The production of documentation is a way of making this knowledge explicit and available to others, at the present and future times. In earlier works, software documentation mainly refers to product manuals. Barker defined software documentation as —the design, planning, and implementation of any interface element, written and online, of a software system to enhance the system's usability. Based on this definition, documentation referred to software product manuals that were written for guiding users to use systems. In this terminology, documentation did not cover the technical documentation used across software development life cycle, e.g., requirements or design documents. (Golara Garousi, a Hybrid Methodology for Analyzing Software Documentation Quality and Usage, September 2012b)

6.2 DIRECTIONS FOR FUTURE RESEARCH

The software will be incorporated with new features to enhance them to be able to answer unsolved technical issues and what is taught to be impossible by I.T. experts.

- Integration of Antivirus software to make the security part of the software complete to the task thereby protecting the network from Phishing, worms, virus, trojans and brute man force attack.
- The ability to respond and act in real time to an activity alert is always the best, SMS and e-mail alert will be incorporated into the software. The email is not only going to depend on internet but in case the users don’t have internet service on the phone to receive the alert it will be converted to SMS format.
- In terms of violation the administrator should gain some evidence on the track of user activity and also be able to back it up to an online web server at a remote location which only a top management user can have access to .This will make it more authentic and evidence cannot easily be compromised.
- Email tracking and real time transmission tracking of information in reader format that only the administrator can have that format and any other intruder will have it encrypted.

6.3 RECOMMENDATIONS

The software is recommended for any organization that uses a computer network. Since it is mandatory for an administrator to know any device connected to his or her network. The software is also good for security systems monitoring which will detect intruders and the software can shutdown machines that are far away or machines that are unwanted do work at a particular time. It is easy to track malicious users through MAC address identification, since MAC addresses are unique on every machine. Time management is an essential tool for an

I.T. personnel due to this fact the software have an option that logs all processes of the monitoring for the administrator to review past events of the monitoring software.

- One difficult part of remote assisting is being able to detect physical I.P. of a remote system due to this fact the software is able to detect all connected I.P's and makes it easier for remote management.
- The software has the ability to track all printers and shared folders which have been created and shared. Since some users do share resources without authorization.
- Being able to detect an external user in your network is also another difficult task, the software have an in built tracking using tracert to locate the hop count of the user to determine how far the user is.

6.4 GENERAL CONCLUSION

The following conclusions were made from the findings.

- It was observed that system administrators were able to do real-time monitoring with the software.
- System administrators also expressed much appreciation because the software possesses ability to actively perform events and actions on the network.
- The software possesses better troubleshooting capabilities to test for connectivity of users or nodes on the network.ie.using the ping
- It was observed that the software displays actively users on the network.
- Within the shortest possible time when configured on the network, the software displayed the users on the network by machine name and domain they are connected to.

REFERENCES

Austin, R. D., & Darby, C. A. (2003). The myth of secure computing. *Harvard Business Review*, *81*(6), 120-126.

Eddy, N.(2014): Associate Editor. Retrieved from http:// www.eweek.com (accessed on 30th January, 2014).

Doug, B. (2012). Security Onion. Retrieved from http://securityonion.blogspot.com/

Hallawell, A. (2004). Re-evaluate the Privacy Risks of Hosting Data in the U.S. A published Gartner report.

Halse, A.G (2003a): Novel Approaches to the Monitoring of Computer Networks

Halse, A.G (2003b): Novel Approaches to the Monitoring of Computer Networks

Halse, A.G (2003c) :Novel Approaches to the Monitoring of Computer Networks

Garousi, G.(2012a). A Hybrid Methodology for Analyzing Software Documentation Quality and Usage

Garousi, G. (2012b). A Hybrid Methodology for Analyzing Software Documentation Quality and Usage

Feamster, N. and Balakrishnan, H.(2005). Detecting BGP Configuration Faults with Static Analysis. In *Proc. 2nd Symposium on Networked Systems Design and Implementation*, Boston, MA.

Rackl, G. (2001). *Monitoring and managing heterogeneous middleware* (Doctoral dissertation, Technische Universität München, Universitätsbibliothek).

Rasmussen, S. (2002). Centralized Network Security Management, Combining Defense in Depth with Manageable Security, SANS Institute Security Reading Room, Retrieved May, 2014, from http://www.sans.org/ reading room/).

Schneir, B. (2005a), Managed Security Monitoring: Network Security for the 21st Century.

Schneir, B. (2005b) Managed Security Monitoring: Network Security for the 21st Century.

Wang, H., Wang, H. H., & Wang, H. H. (1999). *Telecommunications Network Management*. McGraw-Hill Professional.

Webopedia (2013). Software security: http://en.wikipedia.org/wiki/Software. (accessed on 01/11/13)

Yusuff, A.(2013a): Network monitoring, Bachelor's thesis Central Ostrobothnia University of applied Sciences Degree Programme in Information Technology

Yusuff, A. (2013b): Network monitoring, Bachelor's thesis Central Ostrobothnia University of applied Sciences Degree Programme in Information Technology .