Study of Security Issues in the ERP System Implementation And Development of the Security Analysis Tool

D M Sanka Kolitha Dissanayake

139162V

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirements of the Degree of Master of Science in Information Technology

March, 2016

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Sanka 29/04/2016

D.M. Sanka Kolitha Dissanayake Date

The above candidate has carried out research for the Masters dissertation under my supervision.

UOM Verified Signature 29/04/2016

Mr. Saminda Premaratne Date

Dissertation Supervisor

Dedication

This thesis is dedicated to my beloved wife, Dhanushka Priyangi, to my children's Oneli Sethumya and Methum Sethmina they have always encouraged me to do this master degree.

Also this thesis is dedicated to my parents, D M Jayasekara and Lalitha Ekanayake who have given me a tremendous education since beginning of my life, mother in law C. Herath, my brother Ranga and his wife Imali, sister in law Eranga and her husband Dananjaya.

Finally, this thesis is dedicated to all who believe in the richness of learning and value of knowledge sharing among members in communities.

Acknowledgement

This thesis would not have been imagined without kind support and response of many people.

Firstly, I would like to my sincere gratitude to Mr. Saminda Premaratne the supervisor for this project, whose guidance and comments have motivated and improved us throughout the research project. I would also like to kindly thank all of academic and non-academic staff of Faculty of Information Technology, University of Moratuwa, they help us to do our research by conducting a significant lecture series and laboratory sessions throughout the past two years.

The committed and reliable support of my family members have sustained and backed to the accomplishment of this thesis. I am very grateful for their support and understanding throughout during the research project.

The support and guidance given by my head Mr. Dinesh Perera is also helped me, who have given some superb support to do this master degree program.

Also I would like to thank all the survey participants who submitted their view point about ERP security. Without there feedbacks this project can't evaluate properly.

I would acknowledge all others who played a part, however small, in the success of this project. I offer my sincere gratitude to all of them. Thank you.

Abstract

There is a growing tendency in the security of an ERP systems. This has resulted in security issues when an implementing an ERP system. Despite many researchers have discovered various solution for the improve ERP system implementation security there are lack of solutions to analysis security issues of Microsoft Dynamics Navision ERP system.

The solution take various inputs parameters related to the ERP systems. Having giving the input system will be analysis the security threats related to ERP system. After the analysis phase system will produce a report; it consists a list of security issues, suggestions and solutions for those identified issues. This solution can be useful to; ERP systems security auditors, ERP systems own organizations, ERP systems implementation organizations or anyone who interested to investigate the ERP system implementation security issues.

System modules are developed using Open Source technology by using Apache as web server, MySQL as a database server and PHP/Perl/Python as scripting language. System uses existing Open Source libraries and security scanning tools to perform security analysis. The over system has been designed to work in platform independent manner. System can be accessible using any modern web browser also the users can access the system by hosting the application on they own or rented LAMP or WAMP server.

Based on the identified security issues online survey questionnaire was design to understand what target audience are really thinking about the ERP systems security. After the statistically analyzing collected data it shows that those identified issues are significant to the ERP systems security. After development of the security analysis tool, it was tested by the target audience by using the test cases. The results show that our solution can evaluated the ERP systems related security issues.

In summary, the proposed security analysis tool offers unique features necessary for the security of Microsoft Dynamics Navision ERP systems. It also overcomes the limitations associated with existing security approaches and enables the protection of the three major components; people, policy and technology.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Description
ERP	Enterprise Resource planning systems
CIA	Confidentiality, Integrity and Availability
MS	Microsoft
SQL	Structured Query Language
PHP	Hypertext Preprocessor
HTML	Hypertext markup language
NAV ERP	Microsoft Dynamics Navision Enterprise Resource Planning system
BI	Business Intelligence
LAMP	Linux, Apache, MySQL, and PHP/Python/Perl
WAMP	Windows, Apache, MySQL, and PHP
Nmap	Network Mapper
DEM	Dynamic Enterprise Modeler
HTTP	Hypertext Transfer Protocol
RSS	Really Simple Syndication
XML	Extensible Markup Language
IT	Information Technology
MRP	Manufacturing Requirements Planning
BYOD	Bring Your Own Device
VPN	Virtual Private Network
OS	Operating System
NAT	Network address translation
phpMyAdmin	PHP based MySQL database management tool
VM	Virtual machine
US-CERT	United States Computer Emergency Readiness Team
ESE	Extensible Storage Engine
EDB	Extensible Storage Engine Database File
libesedb	Library and tools to access the ESE and EDB format
NT	New Technology (Microsoft Windows term)
ntdsxtract	NT directory information extract

Chapter 1

Introduction

1.1 Prolegomena

Exponential growth of security concern related to the ERP industry new dimension of research in to evolution of usage of security analysis tool [11]. Security is a major concern when implementing an ERP system [10]. Nowadays security challenges growth by application or system software, firmware, hardware, firewall, networking devices and users related. If we are not proper mechanism or tools to update our systems, applications or firmware by using the latest security updates exploitation of one of those vulnerabilities could allow a remote attacker to take control of an affected systems or device. Also when ERP system links with many third party applications like payment gateway tools, BI tools or database systems. Attackers can be access the system using those third party application vulnerabilities [07].

This trend has created a research challenge to analysis and forecast NAV ERP system implementation security. At present there are no specific standalone or web application to audit NAV ERP system security.

System modules are developed using popular open source web platform called LAMP stack is considered by many the platform of choice for development and deployment of high performance web applications which require a solid and reliable foundation [16]. It consists of Apache as web server, MySQL as a database server and PHP/Python/Perl as scripting language. System uses existing Open Source libraries and classes to perform numerous security scanning and investigations. The over system has been designed to work in platform independent manner. System can be accessible using any modern web browser also after this tool release to the public users can access the system by hosting the application on the LAMP or WAMP server environment.

The solution take various inputs parameters related to the ERP systems system. Having giving the input system will be analysis the security threats related to ERP systems system. After the analysis phase tool will provide; list of security issues and the list of suggestions for enhance security level of the ERP system. System also provided a facility to scheduling a predefine security scans those scheduled scanning results are alert via email.

This solution can be useful to; ERP systems security auditors, ERP systems own organizations, ERP systems implementation organizations or anyone who interested to investigate the ERP systems implementation security issues.

After the implementation system was tested using test cases those test results are proving our solution was given expected objectives. The identified security issues are analyses using the online survey. After analysis the performed survey data, it shows that those identified security issues are significant to the ERP systems security. Our solution has recorded 73% of positive performance in the quality, efficiency and accuracy of detection of ERP security issues.

1.2 Background and Motivation

ERP systems are used for leading and managing information within an organization; the sales of such system has increased all over the world since the beginning of the 1990's and the evolution is expected to carry on from 2006-2016 [15]. There were many ERP products were started for various business or industries such as Oil and Gas, Health, Finance, Sales, Education, Production and Construction.

Security provided by Information Technology Systems can be defined as the IT system's capability to being able to defend confidentiality and integrity of processed data, provide availability of the system and data, accountability for transactions processed, and assurance that the system will continue to perform to its design goals [17]. ERP system security must be ruled by the same principles as conventional information security. Figure 1-1 shows the main attribute of the information security.

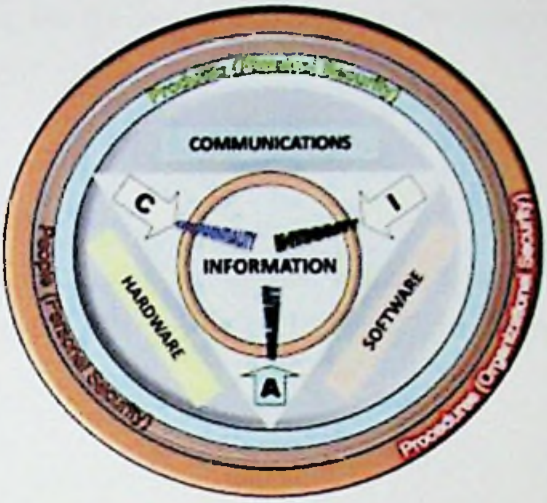

COMMUNICATIONS
C
I
INFORMATION
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Figure 1-1 : Information Security Attributes

Organizations who implemented or planning to implement ERP system are not considering security aspects of implementation or they haven't proper framework, policy or tools for security analysis. This research is motivated to find solutions to the below research questions;

- What are the important security issues in concerns of the RRP system implementation?
- What are the preventive actions or solutions for the identified security issues?
- How to develop a security analysis tool for the NAV ERP?

1.3 Problem Definition

Security is a major concern when implementing an ERP system has been a research challenge. No adequate studies are done in an ERP implementation security and development of security analyses tool for NAV ERP system. Current approaches to enhance ERP security is not enough or mitigate latest threats.

This study will give the best possible opportunity to studying current security issues in relating to the ERP implementation. The approach is based on the premise that information system auditors can use technology to partially automate the process of ERP system security audit. A theoretical model is an automated tool to perform security audits of ERP system, and the concept was validated by implementing and testing in the context of NAV ERP system.

1.4 Aim

The aim of this research project is to study the security issues of ERP implementation and develop a security analysis tool using the identified security issues for the NAV ERP system.

1.5 Objective

Critical review the developments and security issues in ERP implementation study and develop a prototype to automate the NAV ERP system security.

Main objectives of this research project;

- ✓ Study the ERP implementation security issues.
- ✓ Find the most appropriate solutions for the identified security issues.
- ✓ Development of security analysis tool with below modules;
    - ➢ NAV server configurations scanning module.
    - ➢ NAV user permission sets scanning module.
    - ➢ NAV change log auditing module.
    - ➢ User password strength analysis module (MS Active Directory - 2012).
    - ➢ NAV active/inactive user sessions analysis module.
    - ➢ Server open ports analysis module.
    - ➢ Setup and execute automatic security scans.
- ✓ Evaluate the system using test cases and online questionnaire.

1.6 Resources Requirements

Software and Hardware requirements for the development process and running the security analysis tool.

Software requirement for development;

- Microsoft active directory server.
- Dynamics NAV 2013 R2 Server and Client software.
- SQL Server 2012.
- SQL management studio.
- VMware Workstation.
- Kali Linux OS.
- LAMP server.
- Adobe Dreamweaver.
- phpMyadmin.
- Nmap software to perform port scanning.
- Cron daemon tool.
- LimeSurvey as Survey building tool.
- Microsoft Visio.
- Word processing and spreadsheet software.

Hardware requirement for development and running the system;

- Pentium IV or higher CPU.
- 8 GB of physical memory.
- 50 GB of free disk space.
- Interment connection.

Software requirement for running the system.

- Modern web browser

1.7 Structure of the Thesis

The rest of the thesis is structured as follows, Chapter 2 is on critical review of the area of ERP implementation security issues, Chapter 3 presents technology adapted towards an ERP implementation security analysis tool development, Chapter 4 provides the overall picture of the novel approach of ERP implementation security analysis tool, Chapter 5 discuss the design of the solution, Chapter 6 about the implementation of ERP security analyses tool about hardware, software platform, an algorithm and flow charts related to the implementation of the design, Chapter 7 reports on the evaluation of the prototype solution, Chapter 8 conclusion the thesis with note on future works.

Chapter 2

Security Issues of an ERP Systems Implementation

2.1 Introduction

In the Chapter 1 described an introduction, it consists of background information related to this research project. This chapter will discuss about some of the completed research work on the field of study and previous academic research in this field by various parties.

2.1.1 Components of an Information System

According to the Whitman and Mattord security is describe as "the quality or state of being secure – to be free from danger". They explain different layers of security [01].

- **Physical security:** to protect physical objects from unauthorized access and/or misuse,
- **Personal security:** to protect individuals who are authorized to access the system,
- **Operations security:** to protect operations,
- **Communications security:** to protect communication media and contents,
- **Network security:** to protect networking elements, links and contents,
- **Information security:** to protect information assets.

An information system is divided into six components namely hardware, software, data, people, procedures and networks [01]. All these components facilitate information in any information state. [01].

2.1.2 Facts about ERP Systems

ERP which is defined as the capability to provide an integrated collection of business applications. ERP tools share a common process and data model, covering broad and deep operational end-to-end processes, such as those found in finance, HR, distribution, manufacturing, project management, sales, service and the supply chain. [02].

2.1.3 Definition of ERP

A process by which an organization accomplishes and incorporates the key parts of its industry. An ERP management information system integrates areas such as planning, purchasing, inventory, sales, marketing, finance, human resources, project management and etc. [03].

2.1.4 Evolution of ER

ERP is the successor of Manufacturing Requirements Planning (MRP) II. As of industry viewpoint, ERP has extended from direction of manufacturing processes to the combination of enterprise-wide backend processes. From technological side, ERP has grown from legacy implementation to more elastic tiered client-server architecture [04]. Table 2-1 shows the history of ERP systems.

Table 2-1 : History and evolution of ERP [04]

Timeline	System	Description
1960	Inventory Management & Control	Inventory Management and control is the combination of information technology and business processes of maintaining the appropriate level of stock in a warehouse.
1970	Material Requirement Planning (MRP)	MRP utilizes software applications for scheduling production processes. MRP generates schedules for the operations and raw material purchases based on the production requirements of finished goods, the structure of the production

Timeline	System	Description
		system, the current inventories levels and the lot sizing procedure for each operation
1980	Manufacturing Requirements Planning (MRP II)	MRP II utilizes software applications for coordinating manufacturing processes, from product planning, parts purchasing, inventory control to product distribution.
1990	Enterprise Resource Planning (ERP)	ERP uses multi-module application software for improving the performance of the internal business processes. ERP systems often integrates business activities across functional departments.

2.1.5 Characteristics of ERP

- Modular, Flexible and Open Design.
- Central Common Database.
- Automatic Generation of Information.

2.1.6 Benefits of ERP

Investments accomplished by systematizing one system to achieve several business functions, usage of ERP potentials far additional. With a successful implementation of an ERP system, top management can have a consolidated view of Projects, Sales, Inventory, Payables, Receivables, Human Resource related live reports instantly.

- Improved visibility.
- Reduced operating costs.
- Standardized business processes.
- Improved compliance.

2.1.7 ERP Limitations

Implementing an ERP system in a new industry can be very effective. Implementing the same system in an older industry can be very challenging. All employees must be trained, and there will be substantial down time as the business switches all applications over to the new system [05].

- ✓ Policy Limitations

  ERP systems do not fit the business plans of every enterprise. Often, ERP systems must be customized to allow for specific tasks. Not all ERP systems allow this depending on the system or company the business uses, it may be against policy to make such drastic changes to the application.

- ✓ Ongoing Support

  Support for ERP systems often can be difficult to depend on. Technical response can be adept at dealing with minor problems, but major complications with the ERP systems can be beyond the limited customer service available to businesses.

2.1.8 ERP Risk Factors

- ➢ Management Risk
- ➢ Technology Risk
- ➢ Operational Risk
- ➢ Financial Risk
- ➢ Ineffective strategic belief and strategic preparation
- ➢ **Security issues**
- ➢ Legal and regulatory risks
- ➢ Multi-site issues

2.1.9 Example ERP Security issues and vulnerabilities

- CVE-2010-2011

  Microsoft Dynamics GP uses a substitution cipher to encrypt the system password field and unspecified other fields, which makes it easier for remote authenticated users to obtain sensitive information by decrypting a field's contents [21].

- CVE-2010-2083

  Microsoft Dynamics GP has a default value of ACCESS for the system password, which might make it easier for remote authenticated users to bypass intended access restrictions via unspecified vectors [06].

- Chinese attack on USIS using SAP vulnerability.

  On 11th of May 2014, a security headline broke out in the news, it was about an attack on USIS (U.S. Investigations Services) conducted potentially by Chinese state-sponsored hackers via a vulnerability in SAP Software. Hackers broke into third-party software in 2013 to open personal records of federal employees and contractors with access to classified intelligence, according to the government's largest private employee investigation provider [07].

- SAP Afaria vulnerability: One SMS to wipe and lock 130m+ mobile devices of enterprises.

  These issues can be exploited to obtain control over all mobile devices associated with a company via the Internet, as well as wipe and lock them via one SMS message [08].

- Microsoft Dynamics CRM Affected by Self-XSS Vulnerability.

  The vulnerability, identified by researchers at High-Tech Bridge, affects Microsoft Dynamics CRM 2013 SP1 and it can be exploited for XSS attacks against authenticated users [09].

2.1.10 Important Security Risks and Threats related to the ERP

- Sensitive data loss.

- Direct entering of transactions.
    - Update a bank account numbers
    - Change an application password

- Misuse of application privileges.
    - Bypass intended app controls
    - Access another user's privileges

- Impact availability of the application.
    - Wipe out the database
    - Denial of service (DoS)

2.2 Similar Research

The literature survey is primarily based on online sources, mostly peer-reviewed articles published in either research journals or conference proceedings. A few publications by ERP vendors, consulting companies, and industry associations are also considered, including those in the form of case studies.

Security has been identified as a major concern when implementing an ERP system. Wei She and Bhavani Thuraisingham has investigated the security for ERP system [10]. Although there are many researchers working in this area and some solutions are provided to better suited the open environment, yet the security mechanism for ERP system has not yet been brought to the open environment for discussion [10].

According to Wei She and Bhavani Thuraisingham's research they are mainly focused on to the study security issue but they not provided security framework, solution or tool for overcome they identified issue.

Marnewick and Labuschagne has identified a security framework for ERP security that can be used to address all relevant security aspects within an organization [11]. They have mapped generic information technology or IT security framework onto the ERP model to provide the organization with a clear understanding of which security issues must be addressed within which ERP component.

David and Yeohoon has identified factors that companies and audit firms are not yet able to tackle the need of ERP security audit [12]. They have identified following issues:

- ✓ The complexity of ERP systems leads to security vulnerabilities.
- ✓ There is a shortage of staff members trained in ERP security.
- ✓ Implementer's pay inadequate attention to ERP security during deployment.
- ✓ **ERP tools for security audit are inadequate. (The main emphasis of an ERP tools is on security configuration and maintenance)**
- ✓ The customization of an ERP systems to firms inhibits the development of standardized security solutions.

A conceptual model of an automated tool was created by David and Yeohoon to perform an ERP security for SAP R/3 ERP system [13].

According to the Ramdas and Amar (2014) research paper published on IJMSSR (International Journal of Management and Social Sciences Research Volume 3, No. 6, on June 2014) they have highlighted the importance of security in the ERP industry. Their study shows that many companies do not give importance to the security of the ERP database settings and information within the system database [42]. They presented the main issues in terms of ERP security issues will creating a considerable problem in the organization as well as their vital and important data. ERP security plays a major role in the organization and take many attackers or hackers to take valuable data at certain level. Their research paper highlighted a list of some important security issues those are not considered by many organizations or are not seen they are dealing with data during the process. Their paper also discussed the countermeasures and concludes that the importance of data security and information protection mechanisms stated in the ERP system. Also some of the basic and simple solution to problems in ERP systems gain protection technologies feel safe for security threats [42].

Whitman and Mattord (2008) has been identified, when organizations attempting to secure their existing systems and networks, they must consult on the current available information security consultants. According to them in order to develop more secure computing environments in the future, these organizations are counting on the next generation of experts to have the correct mix of skills and experience to expect and accomplish the complex information security issues that can be happening in furfure [43].

According to Shivani and Deepak (2012) research paper was explaining a various types of failures that can be happen within the ERP systems and characteristics of those failures and their relationships were explained. Also they have proposed a vulnerability management cycle with various open source and commercial tools. Briefly explaining their paper, they have highlighted the importance of automating alerts or setting a system alarming are the crucial feature to be successful of ERP system security [36]. They have found that authorizing changes at any time increases the chance of distractions and later it becomes as a disaster.

Christopher and Peck (2004), Sheffi and Rice (2005), Rose and Liao (2006) researches reveals that if there is flexibility in a system to allow changes, the system should be flexible enough to incorporate recovery mechanisms also [37, 38, 39]. Findings of Shivani and Deepak (2012) was mentioned a crucial condition is when there is partial damage in the system and if it have speedy recovery is required so that system is safe. According to them in order to enhance resilience, adaptive capacity and hence flexibility should be increased even after a disruption.

Research done by Fiksel (2006) explained that the redundancy within the system can help increase sustainability of a system and hence can pave the way to faster recovery before full damage [40]. Again we analyzing the Shivani and Deepak (2012) research we have found that the ability to predict these interruptions can be one step in taking preventive measures for handling these before these become a reality. This enhances the security of the system. According to them the vulnerability management cycle [41] can be used for monitoring and predicting the vulnerabilities in the system. Also they proposed that the various tools can be used for handling vulnerabilities within the ERP systems [36].

A multi-layer tree model for enterprise systems vulnerability management has been suggested by Wu and Wang (2011) which helps in succeeding the overall security level of organization. There model have briefly discussed the main entries of tree mode those are; planning for known vulnerability, monitoring for vulnerability, analyzing to identify vulnerabilities, mitigating the vulnerabilities and updating the list of known vulnerabilities [41].

However, major limitation of above researches are they have not considered Microsoft Dynamics Navision or NAV ERP related security issues or solution to analysis security issues of NAV ERP. Although there are many researchers working in this area and some solutions are provided to better suited for SAP and BAAN ERP systems.

The above studies show numerous limitations of an ERP implementation security analysis. Among other issues, security auditing tools and frameworks for security audit not exactly suited for our requirements can be highlighted. These issues are summarized in Table 2-2.

Table 1-2 : Limitation and issues of the past research

Research	**Limitation**
Security for Enterprise Resource Planning Systems. [10].	Proposed reason for ERP security issues, but there are no solution or tool to scan or audit security issues.
A security framework for an ERP system. [11].	Proposed framework is appropriate, but there are no solution or tool to scan or audit security issues.
ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution [12].	Mainly focused on SAP R/3 ERP system. Developed tool for SAP R/3 ERP system.
Security Issue and their Countermeasures in ERP Implementation [14].	Some of the countermeasures are suggest overcoming identified problems but there are no solution or tool to scan or audit security issues.

2.3 Compare with Similar Solution

After the literature survey we found that existing security analysis tool developed by Fastpath Inc. it has following security scanning modules;

- **Assure for NAV**

  Risk based security access review and SOD analysis platform.

- **Audit Trail for NAV**

  Continuous monitoring solution that tracks all changes to critical data inside of Dynamics NAV as well as SQL.

- **Audit View for NAV**

  Report design and scheduling tool allows non-technical users to build reports in the Table 2-3 we compare our solution with Fastpath Inc. solution.

Table 2-3 : Compare with similar solutions

#	Security Audit Type	Our Solution	Fastpath Inc
1	Audit Trail and View for NAV	Available	Available
2	Risk based security access review and SOD analysis	Available	Available
3	NAV server configurations scanning	Available	N/A
4	ACTIVE / INACTIVE user sessions analysis	Available	N/A
5	NAV user password strength analysis (AD server)	Available	N/A
6	Server open ports analysis	Available	N/A
7	Setup and execute automatic security scans	Available	N/A

2.4 Problem Definition

Security is a major concern when implementing an ERP system has been a research challenge. No adequate studies are done in an ERP implementation security and development of security analyses tool for NAV ERP. Current approaches to enhance ERP security is not enough or mitigate latest threats.

Based on the literature review so far an ERP implementation security is a major challenge when implementing an ERP system. During the literature survey identified security issues are summarized in Table 2-4.

Table 2-4 : Identified security issues

#	People related identified security issue	Policy related identified security issue	Technology related identified security issue
1	Strength of computer logon password	User, systems and devices password policy	Application/Firmware patch management issues
2	Given system logon details to third party people or another employee	User rolls and privileges policy	Network /System security issues
3	Forget to logoff or lock computer when leaving the workplace	BYOD devices policy	Firewall/VPN configuration and credential issues
4	Social engineering or Phishing attacks	System Incident handling policy	Third party application vulnerability
5	Users can have more than one granted permission	ERP system handling policy	Secure data file storage, transmission and exchange issues
6	Deleting or editing of system data or segregation-of-duty	Third party people related policy	User Identity and access management issues
7	Confidential data stolen or given to third party	Servers or network devices physical and remote access policy	Electronic data retention strategy related issues
8	The bring-your-Own-Device (BYOD) trend	Data Backups, system log file related policy	-

2.5 Summary

This chapter described about literature of Information Security, about an ERP systems and various approaches of other people have study and tested in the field of an ERP implementation security. It includes the details of these different approaches and what technologies they used in achieving their goals. This chapter also reviews the weaknesses and incompleteness's of the approaches considered above. Chapter 3 describe the adopted technologies for development of security analysis tool will be taken in to consideration.

Chapter 3

Technology of ERP Security Analysis Tool

3.1 Introduction

In the Chapter 2 presented security issues faced when the implementation of ERP system and similar researches done by various people.

This chapter will present technology of an ERP security analysis tool development by describing about benefits, how and why Open Source technology can help to develop this tool.

3.2 Benefits and Usage of Open Source Technology

Open source software is software in which the source code used to create the program is freely accessible for the community to view, modify, and re-distribute. There are many software's available as Open Source the including OS (e.g., Linux, Unix), databases (e.g., MySQL, PostgreSQL), productivity tools (e.g., LibreOffice, open office), games, medical, scientific application are available even programming languages like C, C++, PERL, PHP, Python, Java and many more [24].

3.2.1 Kali Linux

Security analyzing tool will be developing by using Kali Linux, it is a Debian Linux based distribution pointed penetration testing and security auditing. Kali has several hundred tools aimed at various information security tasks, such as penetration testing, forensics and reverse engineering. Kali Linux is developed, funded and maintained by Offensive Security, a prominent information security training firm. [25]

Our system was developed under the Kali OS. After configuring the LAMP server on top of the OS we have installed phpMyAdmin to handle MySQL database and other relevant tools finally we have started development work using PHP scripting language.

3.2.2 LAMP Stack

Our security analysis tool was running top of the LAMP stack, it is considered by many the platform of choice for development and deployment of high performance web applications which require a solid and reliable foundation [16]. It consists of Apache as web server, MySQL as a database server and PHP/Python/Perl as scripting language. LAMP is running under Linux OS but when users required to use those applications on Windows computer they can use WAMP.

Main reasons for choosing LAMP stack to develop this application:

- ✓ Runs under the Linux OS.
- ✓ Fast and have higher performance.
- ✓ Can integrate various Linux based security modules.
- ✓ Web based solution can access using any web browser.
- ✓ All the development tools are freely available including the OS.
- ✓ Using PHP, it can connect to the MySQL and SQL servers.

3.2.3 Apache HTTP Server

Apache is Open Source web server. It's very robust, meaning it can handle large capacities of traffic on a single server. Apache can also serve many different kinds of content with minimal configuration. It scales really well. So the same progress offer can serve tiny static sites for the couple requests an hour to large enterprise applications with hundreds of thousands if not millions of hits per day. We used Apache web server to host our software containing PHP, XHTML, JavaScript's and CSS files [28].

3.2.4 MySQL Database Server

MySQL is the most popular open source database. With its recognized performance, reliability and easiness of use, MySQL has turn into the select of prominent database for Web based applications [29].

We used MySQL as database server to store data related to the security analysis tool MySQL database hold all the data related to the various scans, system credentials and master data related to security scans.

3.2.5 PHP Scripting Language

PHP is a well-known and popular Open Source general-purpose scripting language used for many purposes it was mainly used for web application developments. It can be embedded in to HTML pages it is robust, fast scalable and runs under Apache HTTP server [30].

PHP have used as a main language for this solution it was used to perform main scanning modules core task;

- ✓ Lot of PHP extensions were used for perform security cans/audits.
- ✓ It will connect to MSSQL servers to perform NAV ERP scans.
- ✓ Running various Linux tools through PHP.
- ✓ Running Python and Linux shell scripts through PHP.
- ✓ It will help to write all MySQL queries for system function.

3.2.6 MySQL Database Management Using phpMyAdmin

phpMyAdmin is an Open Source software tool written using PHP language, it is to treat the management of MySQL over the web browser. phpMyAdmin supports a wide range of operations on MySQL and MariaDB. Common operations; managing databases, tables, columns, relations, indexes, users, permissions can be done through the user interface, whereas you still have the facility to straight execute any SQL statement.

We have use phpMyAdmin to create and manage our MySQL database that was used to manage system data.

3.2.7 LimeSurvey

To analyzing project related data collected through the surveys and interviews we used LimeSurvey it is an open source on-line survey application written in PHP language on a MySQL, PostgreSQL or MSSQL database, it distributed under the GNU General Public License [18]. As a web based software it enables users using a web interface to develop and distribute on-line surveys, gather responses, generate statistics, and transfer the resulting data to other applications. After installation users can access it using a web browser. Users be able to use rich text in questions and messages, using a rich text editor, and images and videos can be included into the survey [19] [20].

- ✓ LimeSurvey also provides basic statistical and graphical analysis of survey results [21].

3.3 Virtual Machine Technology

When we required to perform security scanning of the NAV ERP system, we required to have two different OS running same time by two different computers/servers or as one OS as host and other one as guest OS using a virtual machine technology [26].

We have used VMware workstation as virtual machine software. It was installed under Windows OS. Kali Linux distribution was installed as guest OS under the VMware workstation, using NAT methodology we can communicate between two OS [27]. By using the VM technology we can perform our testing purpose through single computer.

3.3.1 VMware Workstation

The ERP system was running under the Windows OS. In order to demonstrate the solution, it required to have Windows computer and Linux Computer but using virtual machine technology we configured Kali Linux OS as a development environment.

3.4 Dynamics NAV ERP System

We have used Microsoft Dynamics NAV 2013 R2 software version for our security investigation purpose it was running under Microsoft Windows 7 64-bit OS it consists of ERP server and client software. It uses windows active directory for user authentications and Microsoft SQL Server 2012 server as a database. Appendix A show NAV ERP architecture related graphs.

3.5 Windows Active Directory Server

Microsoft windows server 2012 64-bit edition used to configure active directory and it was used as a user authentication server in the NAV ERP system. It will manage all the ERP users and their ERP passwords.

3.6 Microsoft SQL Server 2012 Server

NAV ERP server uses SQL server to manage data. NAV ERP have NAV administration configuration tool to create ERP server instance using relevant database. SQL database will have kept all data related to the ERP system using more than hundreds of SQL tables. It includes ERP users, there personalization, sessions, change logs, transactions entry, master data and many more in related to the NAV ERP system modules.

3.7 Security Analysis Software Modules

All the above discussed sub sections including 3.2.1 to 3.2.7 are Open source tools and technologies that are used for the development works of security analysis tool. In order gain our objective we have prior knowledge or some experience of those tools and technologies is essential.

3.8 Summary

This chapter described about the technologies involved in this project. The proceeding chapter will discuss about how we took the approach to research and development of NAV ERP security analysis tool to demonstrate our solutions.

Chapter 4

Approach to ERP Security Analysis Tool

4.1 Introduction

Chapter 3 discussed the technology for development of an ERP implementation security issues analysis tool. This chapter present an approach to developing the security analyses tool under several headings namely, input output, process, users and features.

Using the Open Source and LAMP technologies we highlighted the features of our novel approach to ERP implementation security analysis tool development.

4.2 Solutions for the identified security issues

We have explained what the solutions available to mitigate are or minimized the identified security issues for People, Policy and Technology components.

4.2.1 People related identified security issue solutions

Table 4-1 shows the list of security issues related to the People component with solutions.

Table 4-1 : Solutions for people related security issue

#	Identified Security Issue	Solution
1	Strength of computer logon password	Using "User Password Strength" module it can reduce.
2	Given system logon details to third party people or another employee	Using "NAV User Sessions Monitor" module will report this kind of issues.
3	Forget to logoff or lock computer when leaving the workplace	By implementing "User session logout time on the active directory domain policy"

#	Identified Security Issue	Solution
4	Social engineering or Phishing attacks	By educating the employees about this kind of threats.
5	Users can have more than one granted permission	By using the "User Permission Issues" module this kind of issues can be address.
6	Deleting or editing of system data or segregation-of-duty	By using the "ERP Change Log Audit" module this kind of issues can be address.
7	Confidential data stolen or given to third party	By using the "ERP Change Log Audit" module and the implementing firewall rules to restrict file types. This kind of issues can be address.
8	The bring-your-Own-Device (BYOD) trend	By implementing the process and policy to handle BYOS devices this can be address.

4.2.2 Policy related identified security issues solution

Table 4-2 shows the list of security issues related to the Policy component with solutions.

Table 4-2: Solutions for policy related security issue

#	Identified Security Issue	Solution
1	User, systems and devices password policy	By implementing the policy for the "User Password Strength".
2	User rolls and privileges policy	By implementing the policy for the "User rolls".
3	BYOD devices policy	By implementing the policy to handle BYOS devices this can be address
4	System Incident handling policy	By implementing the policy to handle ERP system incident.
5	ERP system handling policy	By implementing the policy to handle ERP system.

#	Identified Security Issue	Solution
6	Third party people related policy	By implementing the policy to handle third party people.
7	Servers or network devices physical and remote access policy	By implementing the policy to handle ERP system related hardware devices.
8	Data Backups, system log file related policy	By implementing the policy for data backup, system files and log handling.

4.2.3 Technology related identified security issue solution

Table 4-3 shows the list of security issues related to the Technology component with solutions.

Table 4-3 : Solutions for technology related security issue

#	Identified Security Issue	Solution
1	Application/ Firmware patch management issues	By regular monitoring the patch or update news bulleting like US-Cert (US-CERT RSS feed was linked on system dashboard)
2	Network /System security issues	By performing "Open Ports Scan" module this issue can be address.
3	Firewall/VPN configuration and credential issues	By auditing the firewall configurations files and scanning it using Nmap tool.
4	Third party application vulnerability	By performing "Open Ports Scan" module this issue can be partially address. Also by updating about latest security threat news this kind of issues can be fix.
5	Secure data file storage, transmission and exchange issues	By implementing the firewall rules to block sensitive data file transmissions.
6	User Identity and access management issues	Using "NAV User Sessions Monitor", "Change Log Audit" and "User Permission" module will report this kind of issues.

#	**Identified Security Issue**	**Solution**
7	Electronic data retention strategy related issues	By implementing the electronic data retention policy related to the ERP system.

4.3 Input to the system

Main inputs are based on the developed security scanning methods those are listed as follows;

- ➢ Security scanning tool user name and password.
- ➢ NAV ERP Servers configuration files.
- ➢ NAV ERP system user permission sets file.
- ➢ NAV ERP change log analysis purpose users can submit relevant users name, date and time, primary key 1, 2 and 3 field values.
- ➢ Active directory server name, IP address, administrative user account name and password.
- ➢ NAV ERP Server and related devices names, IP address and port numbers.
- ➢ Automated security scan schedule date, time, emails and scanning methods.

Input Data Format: Data format can be xml/binary file or alpha numeric values.

Data Preparation: Data should be preprocessed and validated before process

4.4 Output

System will provide bellows outputs

- ✓ List of security issues and the solutions or suggestion based on input data as a report.
- ✓ Security analysis report of overall scanned issues.
- ✓ Automated security issues email.

4.5 ERP System Security Scanning Process

System main process and the technology used for develop the solution will be discussing in this section below Figure 4.1 shows high level process of the security analysis tool.

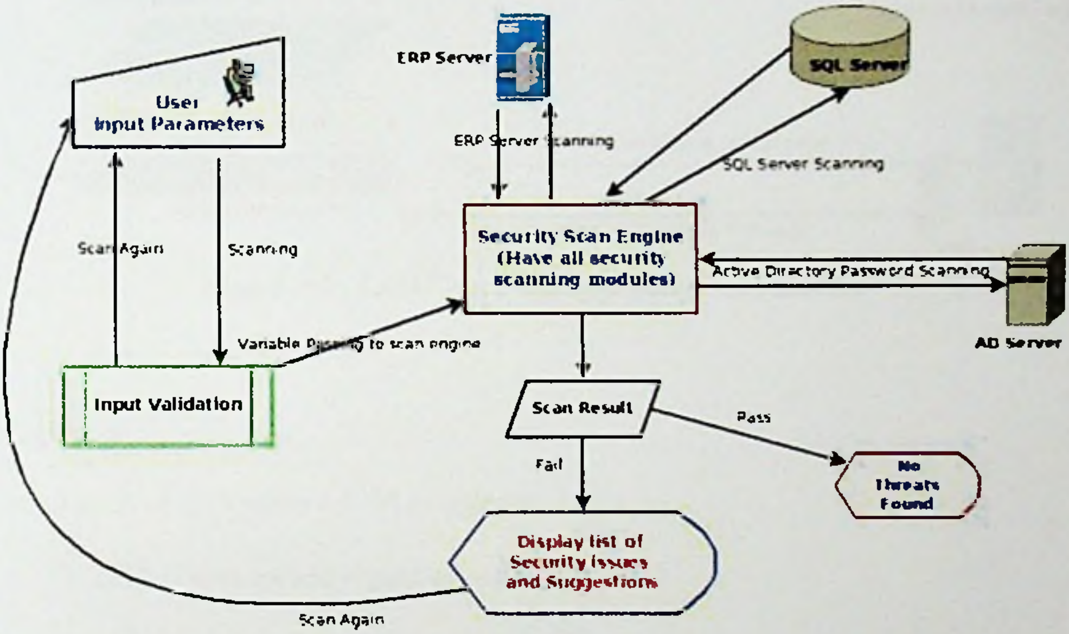


Figure 4-1 : Top Level Process of the Solution

According to the above Figure 4-1 system processes starting based on user input parameters. After user sending data to the system will validate those data and if validation process passed those data will be send to the relevant security scanning module. Then that security module will take the user input parameters and perform security scanning by accessing required ERP system related servers or devices. Finally, if issues are founded system will provide report containing list of security issues and suggested solutions otherwise display there were no issues found.

System modules are developed using popular open source web platform LAMP stack as Figure 4.2 shown below. It consists of Apache as web server, MySQL as a database server and PHP/Python/Perl as scripting language. System uses existing Open Source tools, libraries and classes to perform numerous security scanning and investigations. The over system has been designed to work in platform independent manner. System can be accessible using any modern web browser.

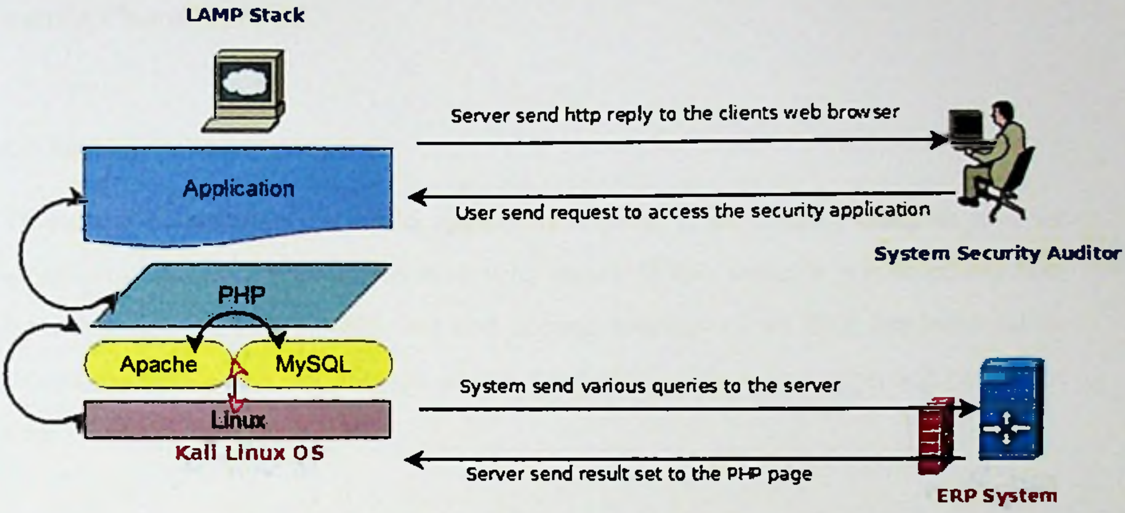

LAMP Stack
Application
PHP
Apache
MySQL
Linux
Kali Linux OS
Server send http reply to the clients web browser
User send request to access the security application
System Security Auditor
System send various queries to the server
Server send result set to the PHP page
ERP System

Figure 4-2 : LAMP stack and application interactions

4.6 Users

Main users of the system are list as follows;

- ✓ ERP system owned organizations.
- ✓ ERP implementation organizations.
- ✓ ERP security auditors.
- ✓ Anyone who like to scan ERP system security issues.

4.7 Features

Main feature of the solution listed below;

- ➢ Scanning security based on the predefined security issues.
- ➢ Security analysis report generation and alert when risk founded via email.
- ➢ System dashboard showing all main functions, security scanning results and latest security threats related data obtaining from the US-CERT releasing live RSS feeds.
- ➢ View list of policy to proceed when implementing an NAV ERP system.

Above list containing core features of the system those are briefly discussed on the coming Chapter 6.

4.8 Summary

This chapter presented our novel approach to develop of security analysis tool for identifying an ERP implementation security issues. In this sense, it is pointed out how the novel approach offers efficient and accrete solution of an ERP implementation security analysis. The next chapter shows the design of the novel approach presented here.

Chapter 5

Design the ERP Security Analyses Tool

5.1 Introduction

Chapter 4 presented the approach to develop a security analysis tool for scanning a security issues of NAV ERP implementation. This chapter elaborate the approach and describe the architecture of the solution. The top level architecture of the solution includes three main modules namely security auditing engine, security analysis report generator and scanning devices/servers data handling components.

5.2 Top Level Architecture

The top level architecture of the ERP implementation security analysis tool. Is shown in Figure 5.1. Within the architecture security scanning engine is the core component of the system and it also shows the interaction with system and ERP system databases.

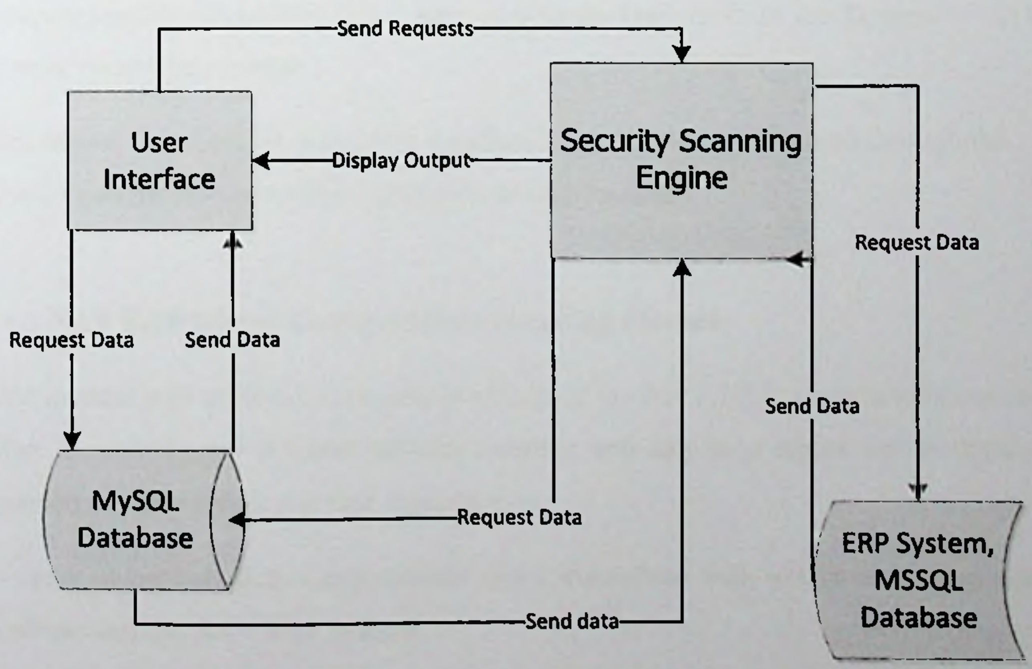


Figure 5-1 : Top level architecture of the ERP security scanning tool

5.3 User Interface

The user interface offers facility to interact with the system for the users, administrators and the developers of the solution. It receives manual entry of information of server/system configuration parameters or automated predefined data through the scheduled scans and send the data to the security auditing engine module for analyses security issues. After analysis input data by the security scanning engine if issues or suggestions found those are display to the user via user interface.

This interface also provides facilities for user authentication, master data management, historical reports view and scheduling automated scans. The interface has been developed as a web application. The interface can access through a web browser.

5.4 NAV ERP Security Scanning Engine

The security scanning engine consist of various kind of security auditing tools, framework/libraries to fulfill the various kind of security issues scanning. Those are containing as a sub module main sub modules are namely NAV ERP server configurations scanning module, Dynamics NAV user permission sets scanning module, Dynamics NAV change log auditing module, ERP user password strength analysis module, Dynamics NAV user session analysis module the Dynamics NAV open ports analysis module.

This engine is connected to the user interface for manual data entry and through the Linux Cron daemon to execute automatic security scans.

5.4.1 NAV ERP Server Configurations Scanning Module

This module will perform a security scanning of the NAV ERP server configuration. After the scanning if it found security issues it will display a report that contains a founded security issues and best suggestions.

In order to perform scans this module make interaction with user interface, system database and the NAV ERP system.

5.4.2 Dynamics NAV User Permission Sets Scanning Module

This module will make communicate with user interface, system database and the NAV ERP system. It will validate that the initially setup user permissions sets by comparing to the current system containing user permission sets data. When module found conflict data related to the user permission sets it will display as a report.

5.4.3 Dynamics NAV Change Log Auditing Module

NAV change log auditing module will interface with user interface, system database and the NAV ERP system. This module will audit the NAV ERP system change log entries data and it will provide a report if it found possible security threats.

5.4.4 ERP User Password Strength Analysis Module

Analysis the ERP system user's password strength. After deep analyzing it will provide a list of report containing strength of password and summary report of analyzed passwords. In order to perform module functionalities, it will interface with all main components shown in Figure 5.1.

Performing AD password audits can help;

- ✓ To identify areas that need enhancement in organization's password policy.
- ✓ Propose metrics that can be used to measure the success of password policy.

5.4.5 Dynamics NAV User Session Analysis Module

This module will analysis the NAV ERP user sessions. If it found potential conflicts, it will be display as a report. This module will interact with all other main modules.

5.4.6 Dynamics NAV Open Ports Analysis Module

This module will interface other modules and scan all open ports of the NAV ERP server and produce a list of reports contains security risk based on open ports and how to avoid them.

5.5 Summary

This chapter presented the architectural design, which will be used to implement the application. In the next chapter the implementation phase of the project will be discussed with further detail.

Chapter 6

Implementation

6.1 Introduction

In chapter 5 the top level design of the solution has been described in terms of what each component does. This chapter describes the implementation of each component regarding tools, hardware, software, algorithms, flow charts and etc. In that sense this chapter is about how the system is implemented.

6.2 Implementation of ERP Security Analyses Tool

ERP security analyses tool has been implemented to run platform independently. It has been developed with LAMP stack it consist of Linux, Apache, MySQL, PHP, PERL and Python as a technology. Let's discuss implementation of individual component details.

6.3 User Interface

The web version of user interfaces is designed using the Adobe Dreamweaver software. The main user interfaces are containing in Appendix B as a user guide.

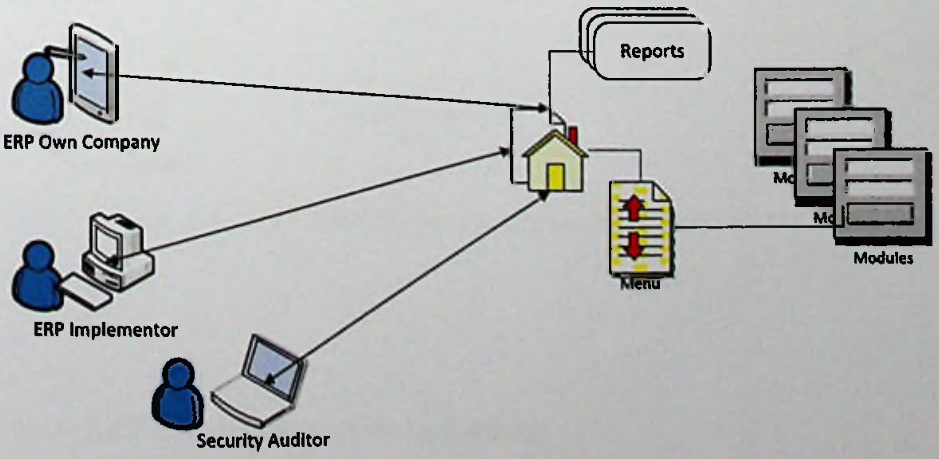


Figure 6-1 : ERP Security Scanning Tool User Interface

Figure 6-1 shown the main user interfaces interaction to the system; using web browser security auditors, ERP implementing people and ERP own organization people can access the web user interface.

6.4 NAV ERP Server Configurations Scanning Module

This module will perform a security scanning of the NAV ERP server configuration. After the scanning if it found security issues it will display a report that contains a founded security issues and the best suggestions for overcome those issues.

Figure 6-2 illustrated the main implementation of this module; this module takes NAV ERP server configuration file and save it to the MySQL database table. Then it performs security scanning by comparing the predefine security rules on MySQL database table. When it detects the issues it will generate a report with list of issues and suggestions.

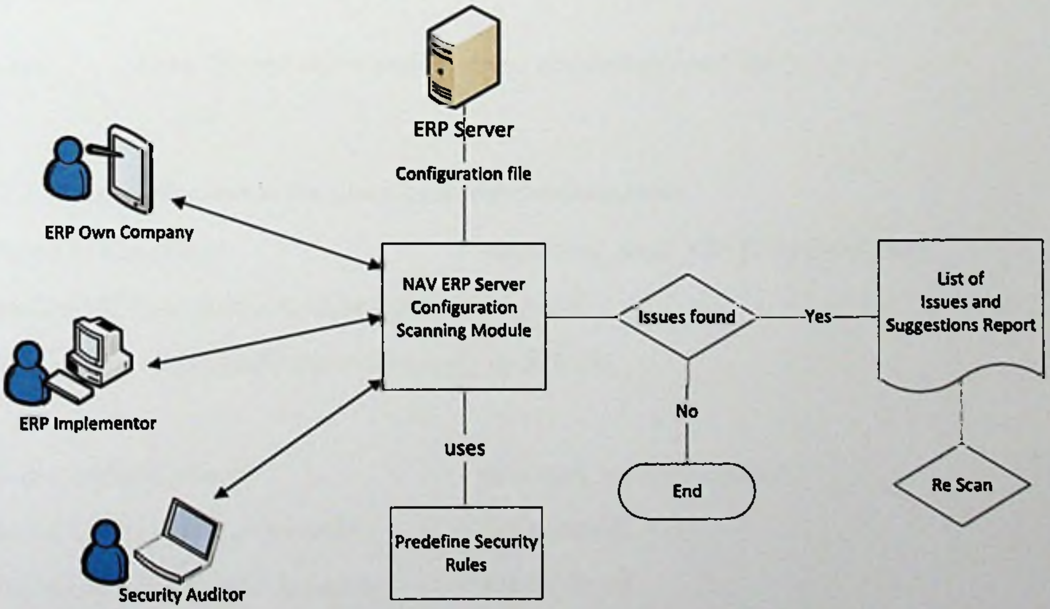


Figure 6-2 : NAV ERP Server Configuration Scanning Module

6.4.1 NAV ERP Configuration File Uploading

Users can upload the NAV ERP server configuration file through the web based form containing under this module. Below PHP code segment used to read file content by temporary uploading file to the server. Then it inserts the contents to the database table. Finally, it will delete the configuration file from uploaded directory.

Below code consist of PHP inbuilt function called *simplexml_load_file()* to interprets an NAV ERP configuration XML file into an PHP object and also *move_uploaded_file()* function to upload configuration file.

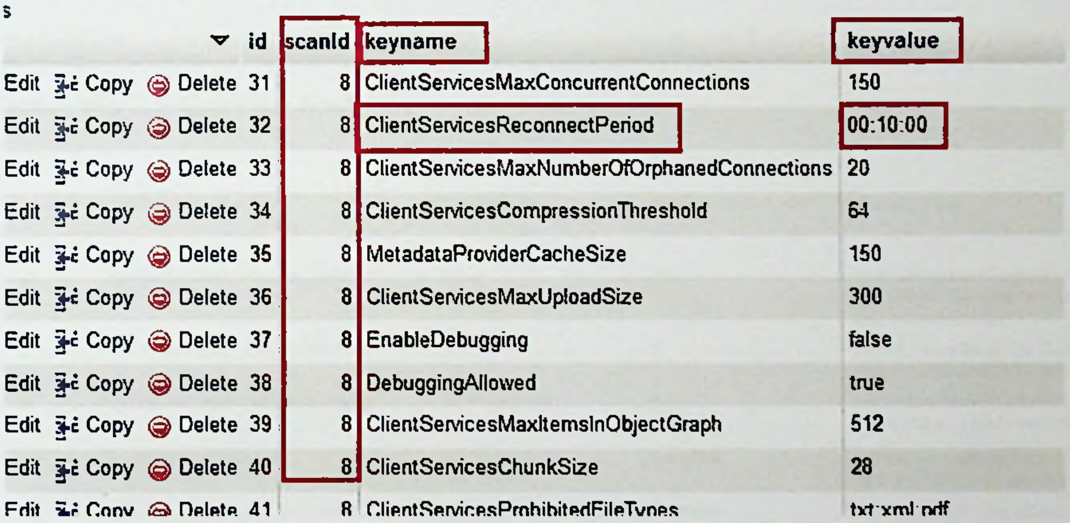
```
//1. File Upload code
$target_dirNavConf   = "Upload/NavServerConf/"; // File uploading folder

$NavConf_file          = $target_dirNavConf.
basename($_FILES["navSRVConf"]["name"]);

 if (move_uploaded_file($_FILES["navSRVConf"]["tmp_name"], $NavConf_file)) {

echo "The Config file ". basename( $_FILES["navSRVConf"]["name"]). " has been
uploaded.";

} else {       echo "Sorry, there was an error uploading your file.";    }


// 2. Insert configuration file contents to the database table
$navSRVConfData                        = simplexml_load_file($NavConf_file);
 include('Classes/class.navConfigFileData.php');
foreach($navSRVConfData->children() as $child)
  {
$navConfigFileData                     = new navConfigFileData();
$navConfigFileData->scanId             =  $insScanId;
$navConfigFileData->keyname            = $child['key'];
$navConfigFileData->keyvalue           = $child['value'];
$navConfigFileData->insert();
  }
```

// 3 Delete uploaded* configuration *file to save disk space

```
if (!unlink($NavConf_file)){  echo "Uploaded file was successfully deleted!";        }
```

6.4.2 Analysis Based on Predefine Security Rules

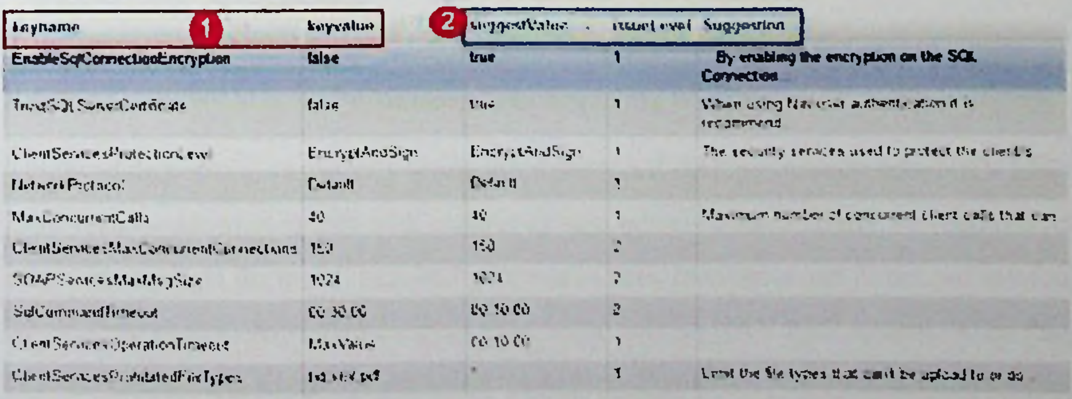
In previous sub section we demonstrate how we upload the configuration file data in to the MySQL table using PHP code segment. In this sub section we demonstrate how we predict the security issues using predefine data set.



	id	scanId	keyname	keyvalue
Edit Copy Delete	31	8	ClientServicesMaxConcurrentConnections	150
Edit Copy Delete	32	8	ClientServicesReconnectPeriod	00:10:00
Edit Copy Delete	33	8	ClientServicesMaxNumberOfOrphanedConnections	20
Edit Copy Delete	34	8	ClientServicesCompressionThreshold	64
Edit Copy Delete	35	8	MetadataProviderCacheSize	150
Edit Copy Delete	36	8	ClientServicesMaxUploadSize	300
Edit Copy Delete	37	8	EnableDebugging	false
Edit Copy Delete	38	8	DebuggingAllowed	true
Edit Copy Delete	39	8	ClientServicesMaxItemsInObjectGraph	512
Edit Copy Delete	40	8	ClientServicesChunkSize	28
Edit Copy Delete	41	8	ClientServicesProhibitedFileTypes	txt;xml;pdf

Figure 6-3 : NAV ERP Server Configuration File on MySQL table

Figure 6-3 illustrate uploaded configuration file in MySQL table.



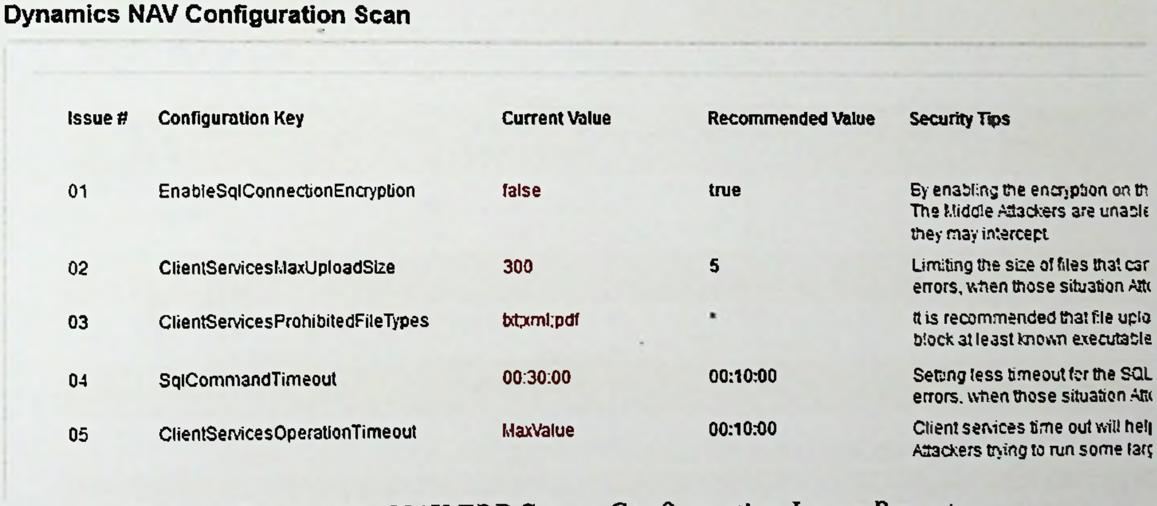
keyname	keyvalue	suggestValue	issueLevel	Suggestion
EnableSqlConnectionEncryption	false	true	1	By enabling the encryption on the SQL Connection
TrustSQLServerCertificate	false	true	1	When using NavUser authentication it is recommend
ClientServicesProtectionLevel	EncryptAndSign	EncryptAndSign	1	The security services used to protect the client's
NetworkProtocol	Default	Default	1	
MaxConcurrentCalls	40	40	1	Maximum number of concurrent client calls that can
ClientServicesMaxConcurrentConnections	150	150	2	
SOAPServicesMaxMsgSize	1024	1024	2	
SqlCommandTimeout	00:30:00	00:10:00	2	
ClientServicesOperationTimeout	MaxValue	00:10:00	1	
ClientServicesProhibitedFileTypes	txt;xml;pdf	*	1	Limit the file types that can't be upload to or do

Figure 6-4 : NAV ERP Server Configuration Rules on MySQL table

Figure 6-4 is a part of MySQL table that stored predefine security rules based on the NAV ERP configuration file, when users running NAV ERP configuration issue report that module have to use this table for prediction of security issues.

6.4.3 Security Issues Report

When users run this report system will provide a report that containing an issues of uploaded NAV ERP configuration file by comparing the predefine standard security rules;



Dynamics NAV Configuration Scan

Issue #	Configuration Key	Current Value	Recommended Value	Security Tips
01	EnableSqlConnectionEncryption	false	true	By enabling the encryption on th The Middle Attackers are unable they may intercept
02	ClientServicesMaxUploadSize	300	5	Limiting the size of files that car errors, when those situation Att
03	ClientServicesProhibitedFileTypes	txt;xml;pdf	*	It is recommended that file uplo block at least known executable
04	SqlCommandTimeout	00:30:00	00:10:00	Seting less timeout for the SQL errors, when those situation Att
05	ClientServicesOperationTimeout	MaxValue	00:10:00	Client services time out will hel Attackers trying to run some larg

Figure 6-5 : NAV ERP Server Configuration Issues Report

Figure 6-5 shown a report that we take from the testing phase; it includes configuration key, current value, recommended value and the security tips.

6.5 Dynamics NAV User Permission Sets Scanning Module

This module performs a security scanning of the NAV ERP permission sets. NAV ERP have various permission sets with various system permissions. Initially we required to create master data for the all required permission sets. In order to get initial permission set, it is required to download existing permission sets on NAV ERP system. After that we can upload them to our system using "Add New Dynamics NAV Permission" menu link. Finally, we can perform security audit based on uploaded permission set. System will compare previously uploaded permission set values and the live server permission sets by accessing NAV ERP MS SQL server through PHP code. If it found security issues it will display a report with all security issues.

Figure 6-6 illustrated the main implementation of this module; this module takes NAV ERP permission set file and save it to the MySQL database table. Then it performs security scanning by comparing with the "[Permission]' table on NAV ERP database. When it detects the issues it will generate a report with list of issues and suggestions

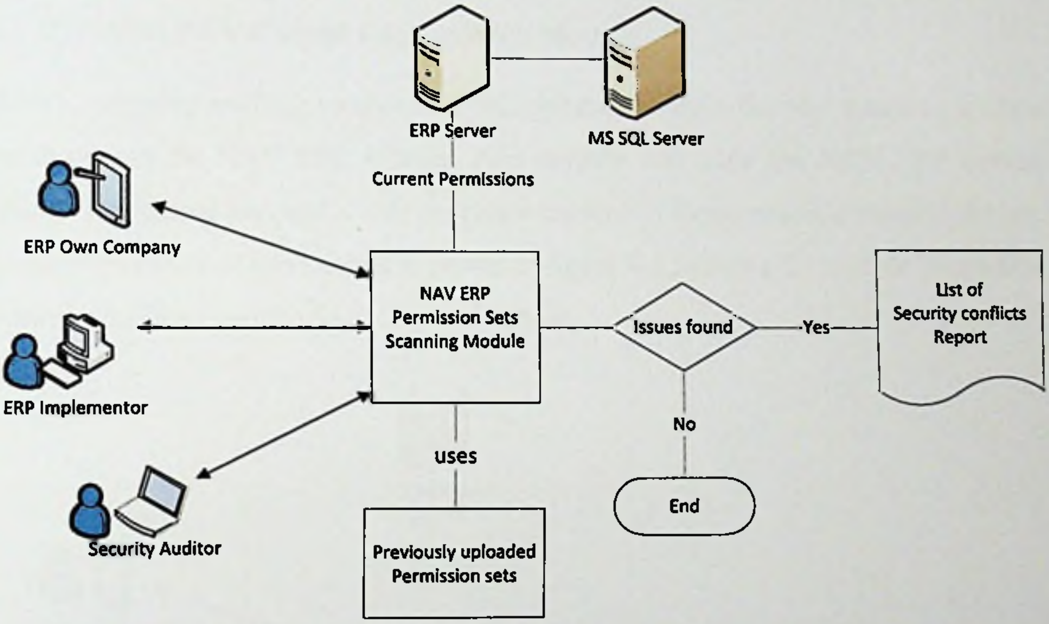
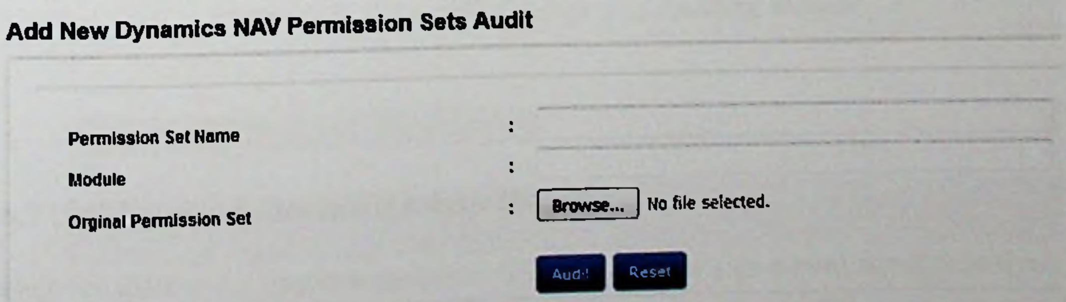


Figure 6-6 : NAV ERP Server Permission Scanning Module

Below figure 6-7 illustrate permission sets data uploading form, it will upload the spreadsheet file with name of the permission set. After that PHP script read the spreadsheet file contents and insert values in to the MySQL database table;


Add New Dynamics NAV Permission Sets Audit

Permission Set Name :

Module :

Orginal Permission Set : Browse... No file selected.

Figure 6-7 : NAV ERP Permission set upload screen

PHP code segment used to connect SQL server,

```
$link = mssql_connect('172.25.1.15\MSSQLSVRPRIMARY', 'xxxxxx, 'pwd');
 if (!$link)    die('Unable to connect!');
 if (!mssql_select_db(ERP_LIVE, $link))
   die('Unable to select database!');
```

6.6 Dynamics NAV Change Log Auditing Module

NAV change log auditing module will take parameters from the user interface, system database and the NAV ERP system. This module will audit the NAV ERP system change log entries data and it will provide a report if it found possible security threats. Main architecture of this module is shown in figure 6-8 it shows the module interaction between end user and the SQL Server database.

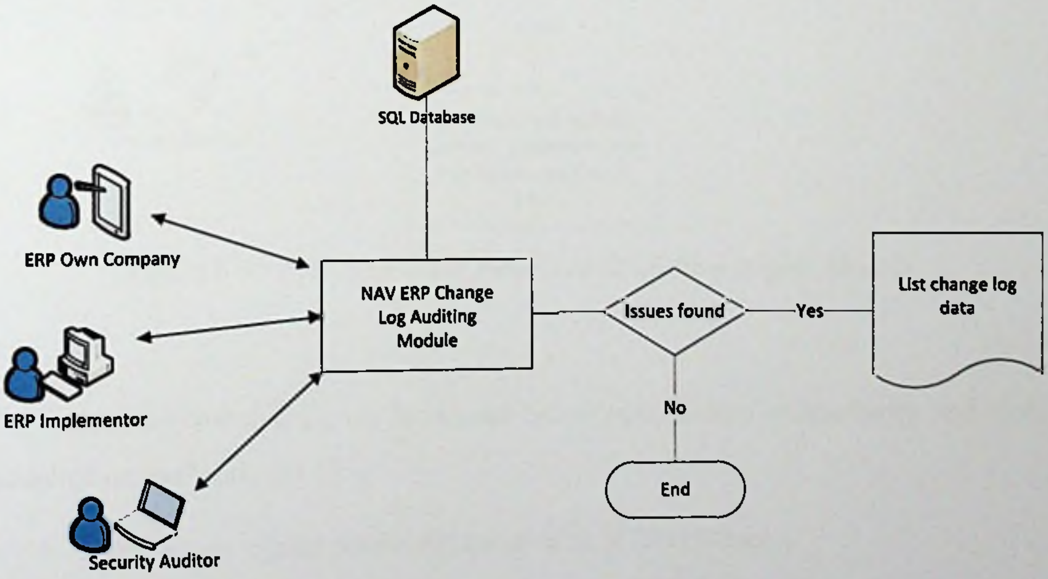


Figure 6-8 : NAV ERP Change Log Auditing Module

6.7 User Password Strength Analysis Module

Here we discuss the implementation of ERP system user's password strength analysis module. This module has required to have access to the Windows AD server to perform password scan. Main architecture of this module is shown in figure 6-9.

Performing AD password audits can help;

- ✓ To identify areas that need enhancement in organization's password policy.
- ✓ Propose metrics that can be used to measure the success of password policy.

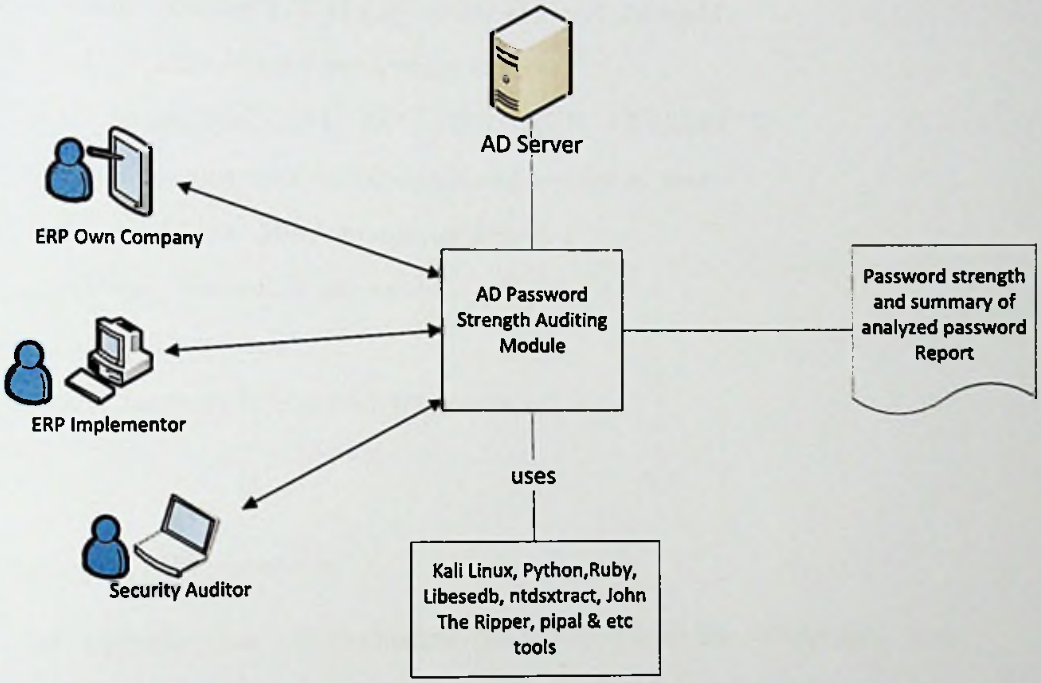

AD Server
ERP Own Company
ERP Implementor
Security Auditor
AD Password Strength Auditing Module
Password strength and summary of analyzed password Report
uses
Kali Linux, Python,Ruby, Libesedb, ntdsxtract, John The Ripper, pipal & etc tools

Figure 6-9 : NAV ERP User Password Strength Analysis Module

For implement this module we have used below open source technologies and tools installed on the Linux OS [33];

- ➢ **Python** – to extract password hashes with NTDSExtract.
- ➢ **Ruby** – Pipal tool developed using ruby language.
- ➢ **Libesedb** - Joachim Metz created library and scripts to interact with Extensible Storage Engine (ESE) Database File (EDB) format.
- ➢ **ntdsxtract** - Csaba Barta's a framework for offline forensic analysis of NTDS.DIT
- ➢ **John The Ripper** - Tries to guess the password by hashing it and comparing hashes.

- **pipal** - Password analysis and presenting tool.
- **shred command** - clean all sensitive files from the system.

Below PHP code segment used to establish a connection with AD server it uses PHP extension called php_ldap;

```
$link = ldap_connect('172.25.1.2'); // AD server IP addredd
if(! $link) {    echo "Could not connect to server"; }
ldap_set_option($link, LDAP_OPT_PROTOCOL_VERSION, 3);
// Now try to authenticate with credentials provided by user
if (! ldap_bind($link, $adUsername, $adPwd)) {
   echo 'error, credentials are wrong';
} else{ echo 'Connected';
//perform password strength scanning here
}
```

Steps of the implementation;

a) Uploading the NTDIS database file obtained from the AD server.

b) Using "*libesedb*" unpack to obtain the NTDIS database tables.

c) Running the "*ntdsxtract*" tool to extract the hashes.

d) Crack the password hashes using "John The Ripper tool."

e) Feeding password hashes to "*pipal*" analytical tool.

f) Clean the used database, hash & output files using "*shread*" command.

Above scenario was implemented on the LAMP technology. After deep analyzing user's passwords, system will provide a report containing strength of password and another summary report of analyzed passwords.

6.8 Dynamics NAV User Session Analysis Module

This module will analysis the NAV ERP database containing "Session Event" table it contains all the user sessions details. We have implemented a method to investigate logon client computer name and user ID values by comparing their relationship. If it found potential conflicts between logon client computer and user ID, it will display as a report. This module will directly access the MS SQL database that NAV ERP system configured. Main architecture of this module is shown in figure 6-10.

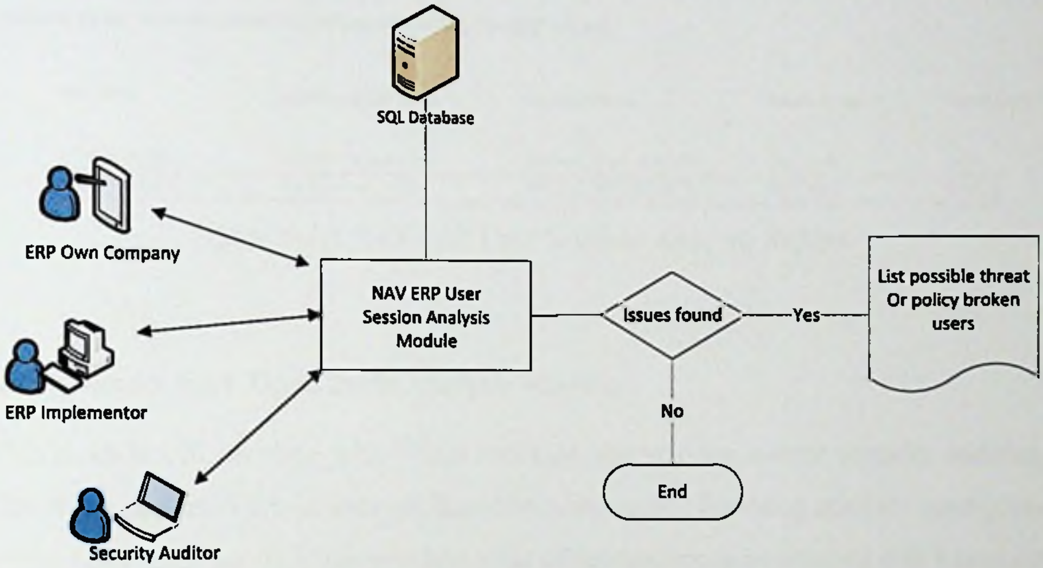
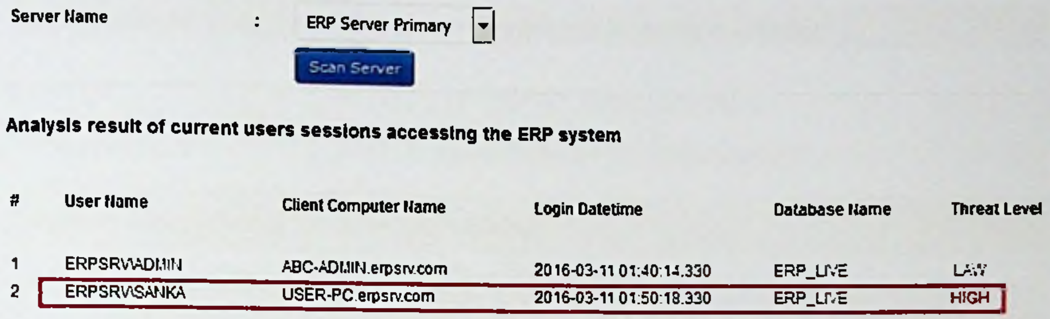

SQL Database
ERP Own Company
ERP Implementor
Security Auditor
NAV ERP User Session Analysis Module
Issues found
Yes
No
End
List possible threat Or policy broken users

Figure 6-10 : NAV ERP User Sessions Analysis Module

Below PHP and MySQL code piece used to investigate possible conflicts of user sessions by comparing user's client computer name this will help us to find segregate of duties or possible internal threats;

```
$sqlChkUserSes = "SELECT [Session ID],[Event Datetime], [Client Type],[Database Name],[Client Computer Name], REPLACE([User ID],'"$DomainName"\',") as 'USER ID'
FROM [Session Event]  WHERE '%' + [Client Computer Name] + '%' not like [USER ID]"
$resultCheck = mssql_query($sqlChkUserSes) or die(mssql_error());
while ($rowRes          = mssql_fetch_array($resultCheck))
{
$dateTime               = $rowRes["Event Datetime"];
$ClientType             = $rowRes["Client Type"];
$DbName                 = $rowRes["Database Name"];
$clientComputer         = $rowRes["Client Computer Name"];
$userName               = $rowRes["[User ID"];      }
```

After analyzing the user session system will produce a report that containing possible considerable user sessions those are highlighting in red color as figure 6-11 shown.



Server Name : ERP Server Primary

Analysis result of current users sessions accessing the ERP system

#	User Name	Client Computer Name	Login Datetime	Database Name	Threat Level
1	ERPSRV\ADMIN	ABC-ADMIN.erpsrv.com	2016-03-11 01:40:14.330	ERP_LIVE	LOW
2	ERPSRV\SANKA	USER-PC.erpsrv.com	2016-03-11 01:50:18.330	ERP_LIVE	HIGH

Figure 6-11: NAV ERP User Sessions Analysis Report

6.9 Dynamics NAV Open Ports Analysis Module

This module will interface with Nmap tool that was an open source security auditing tool it can perform various network based security audits. By using scan all open ports of the NAV ERP server it can produce a list of reports contains security risk based on open ports and how to avoid them. Figure 6-12 shows the architecture of this module.

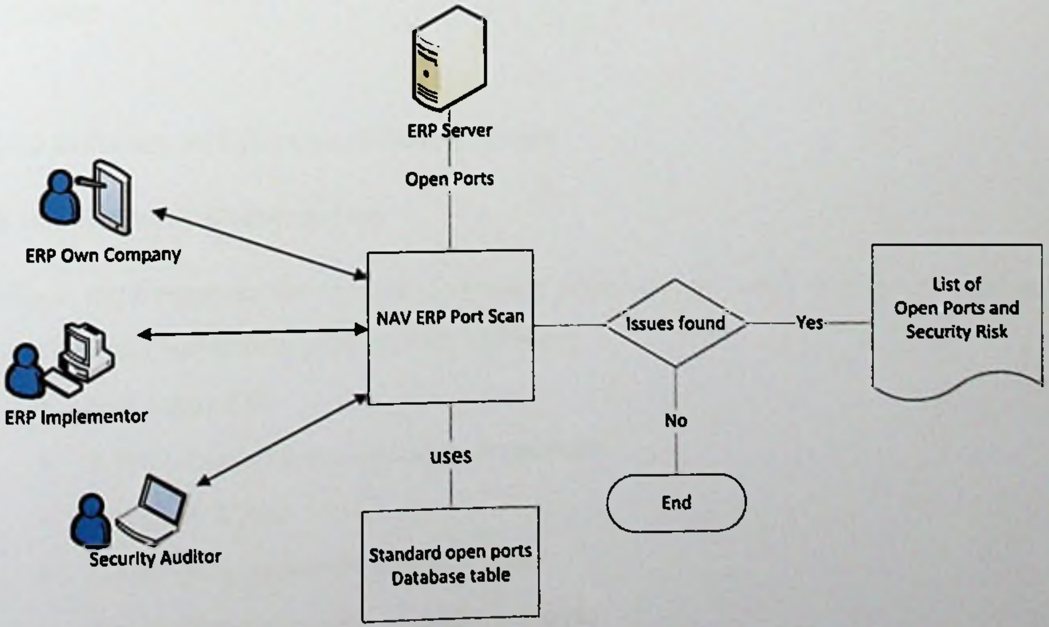


Figure 6-12 : NAV ERP Open Ports Analysis Report

Below PHP code segment was used to access namp binaries and perform a port scan for the user provides IP address and server name [32].

```
require_once 'Net/Nmap.php';

//getting user entered values namp will perform a security scanning

$serverIP              = $_POST["serverIP"]; //post variables
$serverDomain          = $_POST["serverDomain"]; //post variables

$target = array($serverIP, $serverDomain);
$options = array('nmap_binary' => '/usr/local/bin/nmap');

try {    $nmapPortScan = new Net_Nmap($options);

 $nmapPortScan_options = array(        'os_detection' => false, 'service_info' => true
);

$nmapPortScan->enableOptions($nmapPortScan_options); // Scan
$res = $nmapPortScan->scan($target); // get results
```

After above process system will generate a report based on comparing the scan result found open ports with predefine standard open ports list table reside on the MySQL database.

6.10 Software and Hardware Requirements

6.10.1 Software Requirements

When implementing the system following software are used for the designing, development and testing phases of the software.

- Kali Linux OS.
- Word processing and spreadsheet software.
- Microsoft Visio.
- LimeSurvey as Survey building tool.
- Adobe Dreamweaver for interface design.
- LAMP Server Stack.
- phpMyadmin MySQL administration tool.
- Nmap software to perform port scanning.
- Cron software to schedule scanning.

- Windows active directory server.
- Dynamics NAV 2013 R2 Server and Client software.
- SQL Server 2012.
- SQL management studio.
- VMware Workstation.

6.10.2 Hardware Requirement

When implementing the system following hardware resources are used;

- Pentium IV or higher CPU having computer system.
- 8 GB of physical memory.
- 50 GB of free disk space.
- Network card.

6.11 Implementation Challenges and Resolutions

There were certain challenges to face from the research phase up to the implementation. After identified ERP security related issues, proposing a most suitable solution to prevent the identified security issues is take lot of time it is required study the current security analyzing/auditing technologies and also required to test solutions using sample data in real environment.

When we considering some implemented security analysis modules some of audits consume lot of hardware resources; memory, CPU, GPU and disk reads. Also to perform those audits take too much of time as an example when auditing AD server user's password strength, it has required higher system resources and also it take many hours to read AD domain controllers users password hash file. If our system hasn't enough resources when performing those scans system can he hang-up. As a solution for this issue we can perform partial audits or sequential based audits.

With rapid change of Information Technology and Information Security related threats, vulnerabilities, precautions, and approaches to security there is no guaranteed proposed solution will mitigate the identified security issue. By observing latest IT security threats we must update our system to handle those new attacking technologies and tools.

6.12 Summary

This chapter briefed about the implementation of this project. By explaining main modules with suitable example code, flow charts, architectural diagrams, system and database tables screen-shots.

The proceeding chapter will contain how we evaluate the system.

Chapter 7

Evaluation

7.1 Introduction

The previous chapter discussed about how the tool is developed in a step by step process. This chapter will show how solution was evaluating to see whether objectives has been achieved.

7.2 Evaluation Technologies and Tool

Evaluation will help us to check success of the proposed solution by set of predefined goals. This research projects goals are stated on the chapter 1. After the evaluation process we can identify system weakness, good areas and improvements.

We have performed a system testing and online questionnaire for evaluate our solution.

The complete test cases and test result for the NAV ERP security analysis tool is given as Appendix C.

Questionnaire was used to collect information as of several reasons. First, even though the security analysis tool was specifically developed to IT professionals. Second, comparing with other data gathering methods like interview, observation and archival data, questionnaire gives analysts of user's response in real-time and it can also easy to analysis since survey data are stored in the database.

At the very beginning of the study, unstructured questionnaire is applied because it is useful to explore the ERP community members' feedback about how they see ERP security it is given as Appendix D. At the end of implementation to evaluate the solution and tool, well-structured questionnaire is created it is given as Appendix E.

Qualitative measurements are put on to the online survey tool called "LimeSurvey" and after that results are analyses using it. Questionnaire is based on participants group and quality attributes of the system according to the survey it shows that our solution has recorded 73% of positive performance in the quality, efficiency and accuracy of detection of NAV ERP security issues.

System prototype was published on a LAMP server. Link of system with relevant user credentials to access the system was given to the selected IT professionals via email. Also provided them to the link of online survey tool.

7.3 Qualitative Measurements Evaluation

This process was based on an online survey questionnaire. Steps of this evaluation process are:

- Ask a quality or characteristic based questions.
- Obtaining a response and save.
- Analysis the survey result and make prediction.
- According to the survey results change the solution.

7.3.1 Sampling Plan

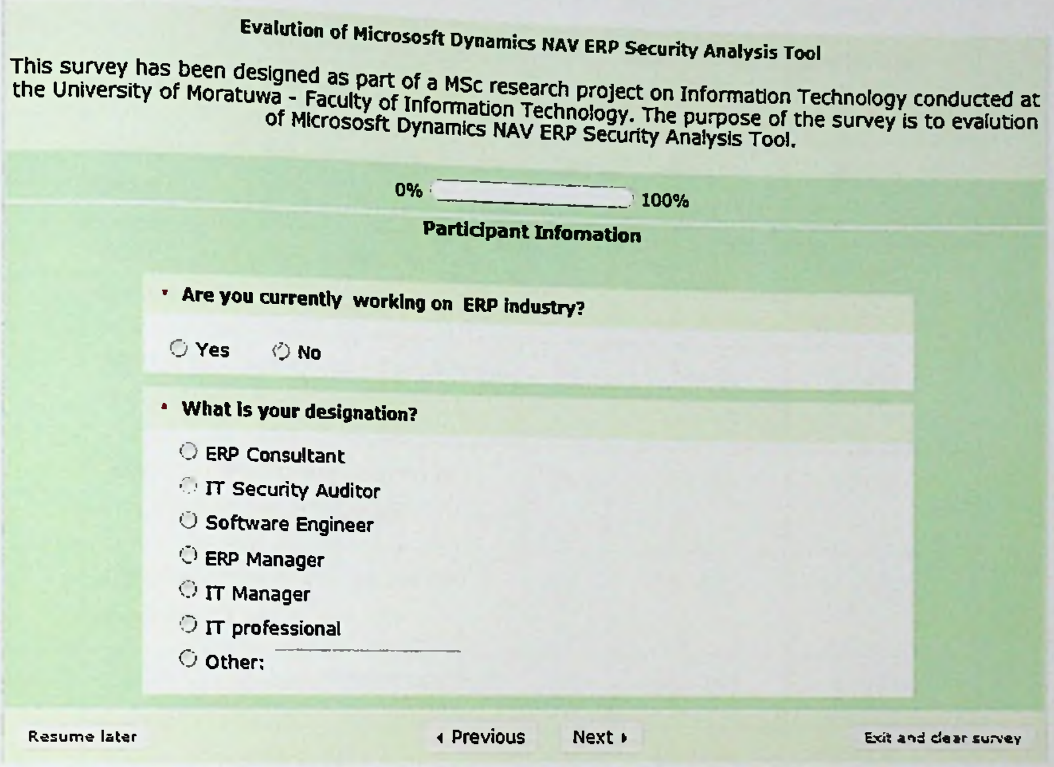
For evaluate the research project objectives, we selected set of people from the categories mention below:

- ERP consultants.
- ERP own or implementing organizations IT staff.
- IT security auditors.
- IT professionals who have knowledge of ERP systems

We have limited people available from each category since NAV ERP was using a few companies and also less than ten NAV ERP implementing parties available within the Sri Lanka.

7.3.2 The Questionnaire

Qualitative measurements are put on to the online survey tool called "LimeSurvey". After completing the survey results are analysis using it. Questionnaire is based on quality attributes of the system. Below figure: 7-1 shows the main scree of survey, the completed survey questionnaire is given as Appendix E.



Evalution of Micrososft Dynamics NAV ERP Security Analysis Tool

This survey has been designed as part of a MSc research project on Information Technology conducted at the University of Moratuwa - Faculty of Information Technology. The purpose of the survey is to evalution of Micrososft Dynamics NAV ERP Security Analysis Tool.

Participant Infomation

* **Are you currently working on ERP industry?**

○ Yes ○ No

* **What is your designation?**

○ ERP Consultant
○ IT Security Auditor
○ Software Engineer
○ ERP Manager
○ IT Manager
○ IT professional
○ Other: ______

Figure 7-1 : Survey Questionnaire Sample Page

7.3.3 Analysis the Results

After completing the survey process responses were analysis using the "LimeSurvey" analysis module. Figure 7-2 to 7-9 shows the analysis of survey results as a graphs. Table 7-1 is showing the result related to evaluation of our solution:

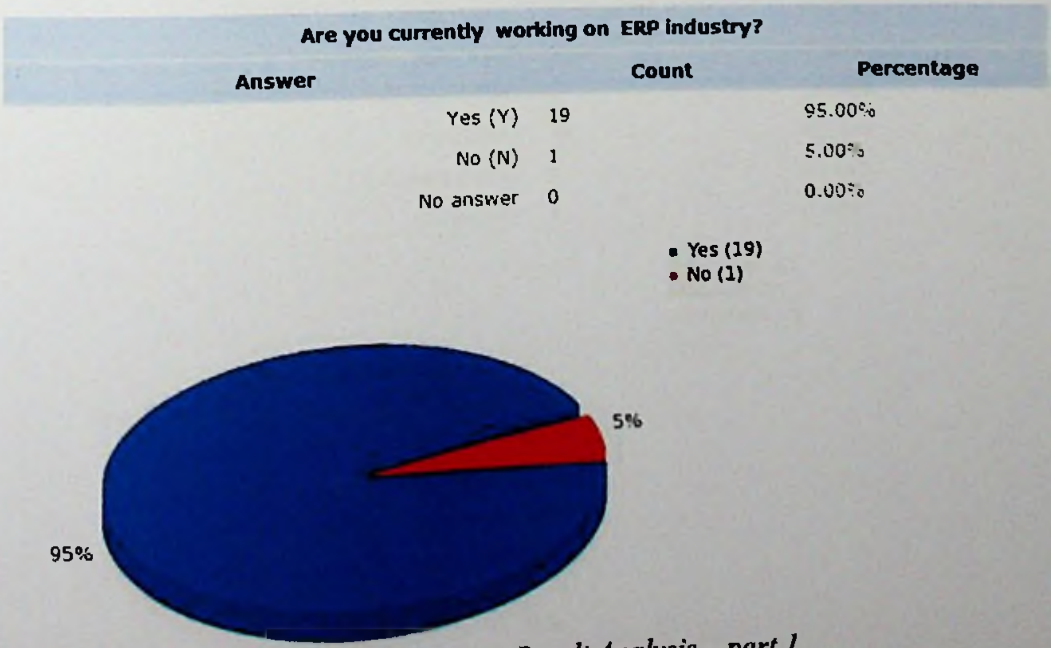
Table 7-1 : Summary of system evaluation survey

Sr. No.	Question	N*	Positive Responses (%)	Negative Responses (%)
1.	How are you rank the user interface of system?	20	17 (85)	5 (15)
2.	How are you rank the response time of application?	20	14 (70)	6 (30)

Sr. No.	Question	N*	Positive Responses (%)	Negative Responses (%)
3.	How you rank the accuracy of result?	20	15 (75)	5 (15)
4.	What is your given quality grade for the exception handling?	20	12 (60)	8 (40)
5.	What is the level of user friendliness of the system?	20	12 (60)	8 (40)
6.	How you rank the importance of security analysis modules?	20	14 (70)	6 (30)
7.	Security analysis tool results and suggestions are?	20	13 (65)	7 (35)
8.	Quality of security analysis reports?	20	15 (75)	5 (25)
9.	Quality of overall system?	20	17 (85)	3 (15)

*Out of total respondents 20, those who did not respond were deleted.

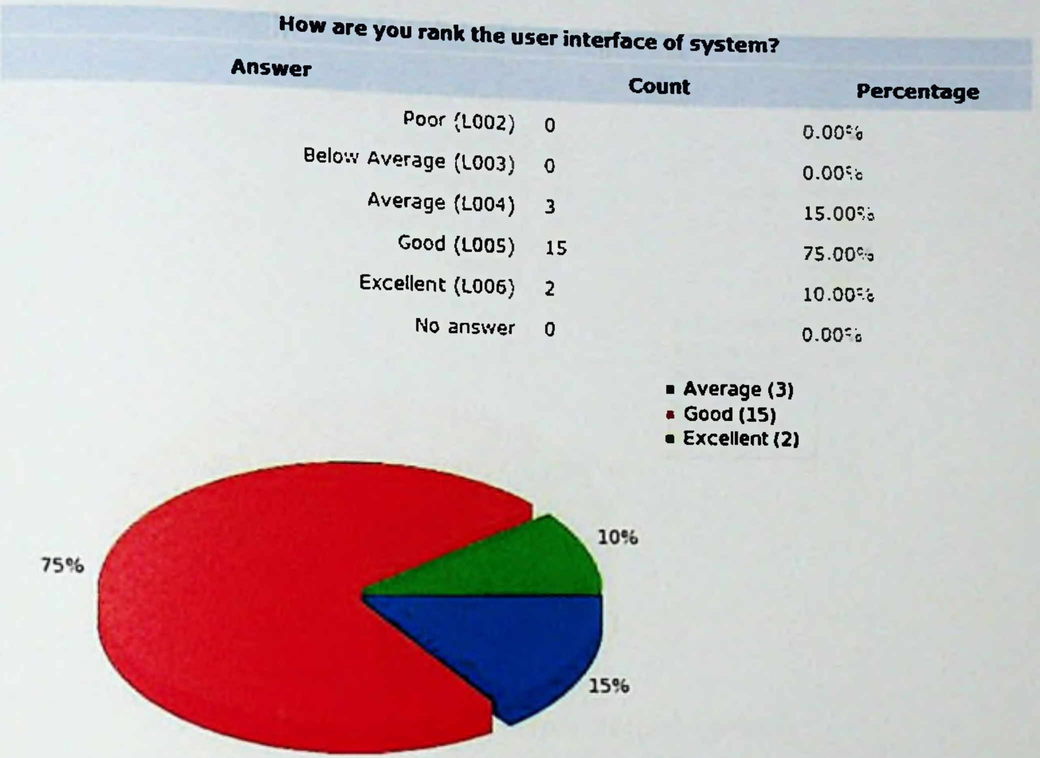
Here we list some answers summary using graphs;



Are you currently working on ERP industry?

Answer	Count	Percentage
Yes (Y)	19	95.00%
No (N)	1	5.00%
No answer	0	0.00%

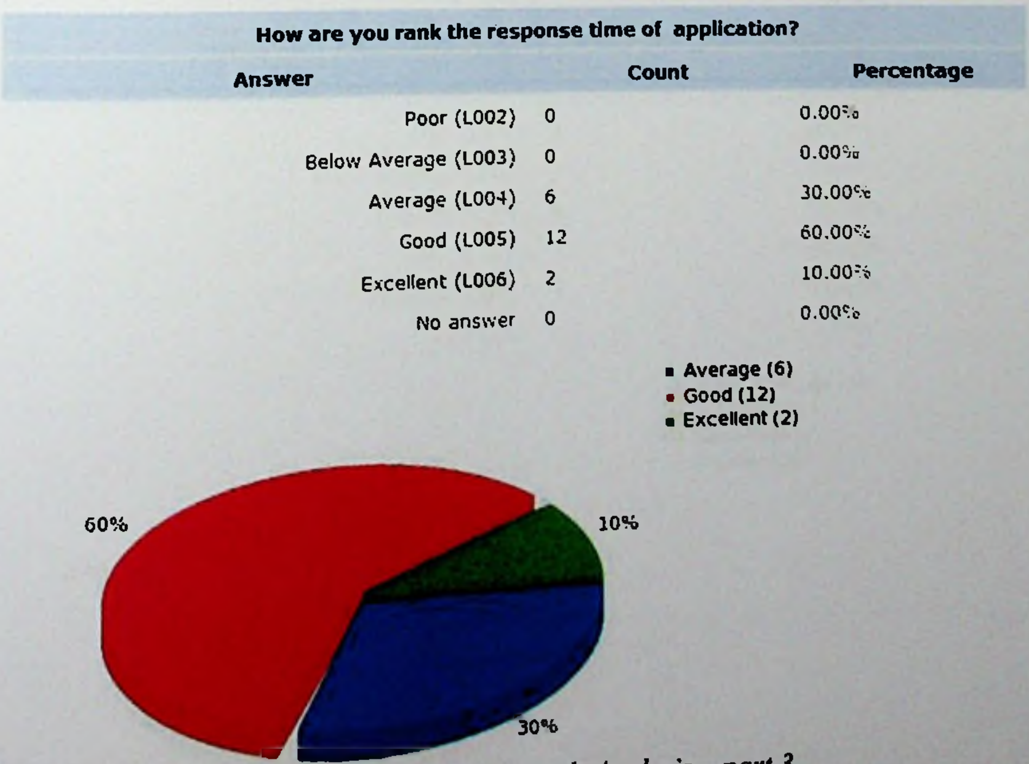
Figure 7-2 : Survey Result Analysis – part 1



How are you rank the user interface of system?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	0	0.00%
Average (L004)	3	15.00%
Good (L005)	15	75.00%
Excellent (L006)	2	10.00%
No answer	0	0.00%

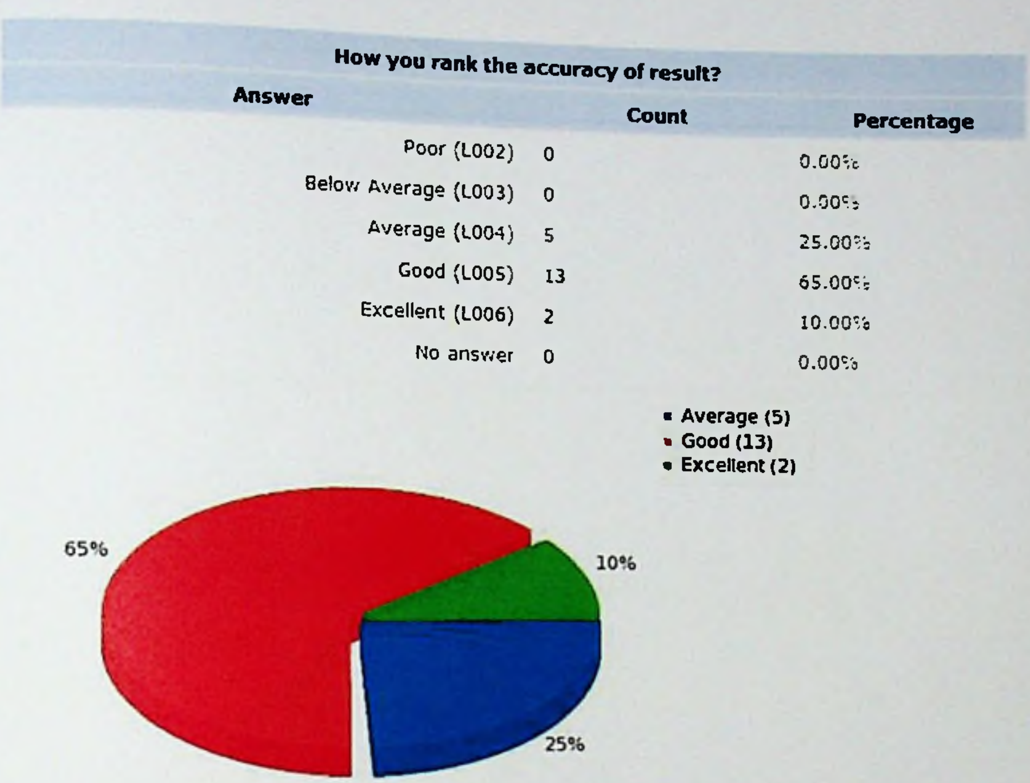
Figure 7-3 : Survey Result Analysis – part 2



How are you rank the response time of application?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	0	0.00%
Average (L004)	6	30.00%
Good (L005)	12	60.00%
Excellent (L006)	2	10.00%
No answer	0	0.00%

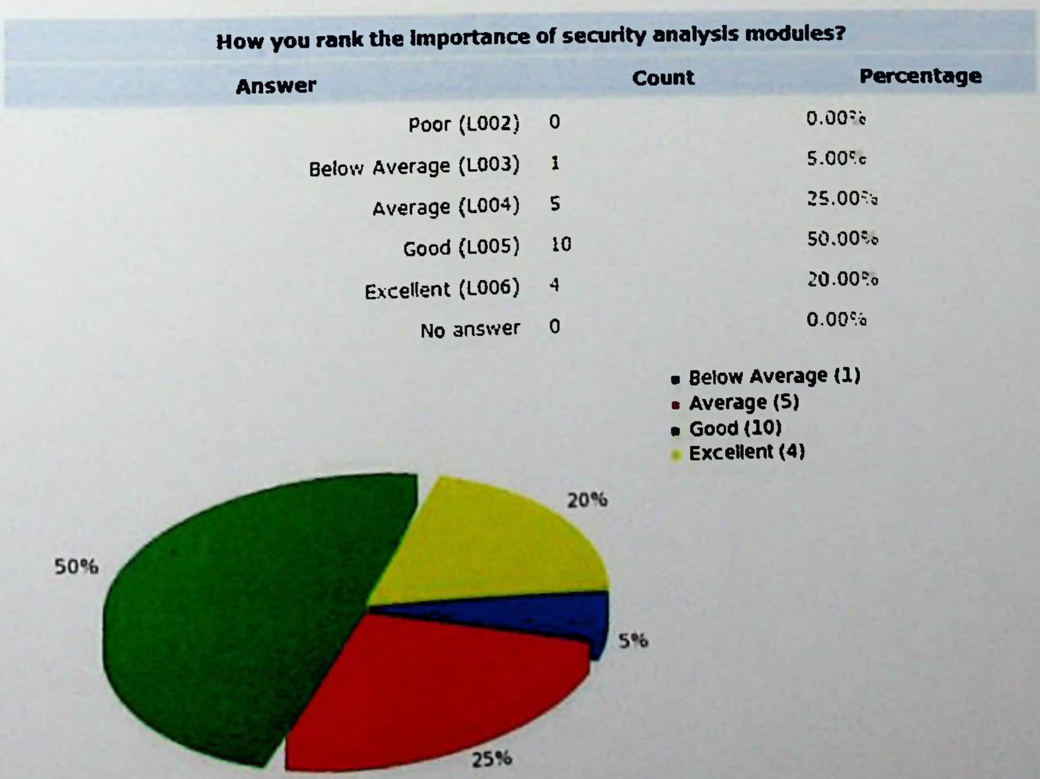
Figure 7-4 : Survey Result Analysis – part 3



How you rank the accuracy of result?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	0	0.00%
Average (L004)	5	25.00%
Good (L005)	13	65.00%
Excellent (L006)	2	10.00%
No answer	0	0.00%

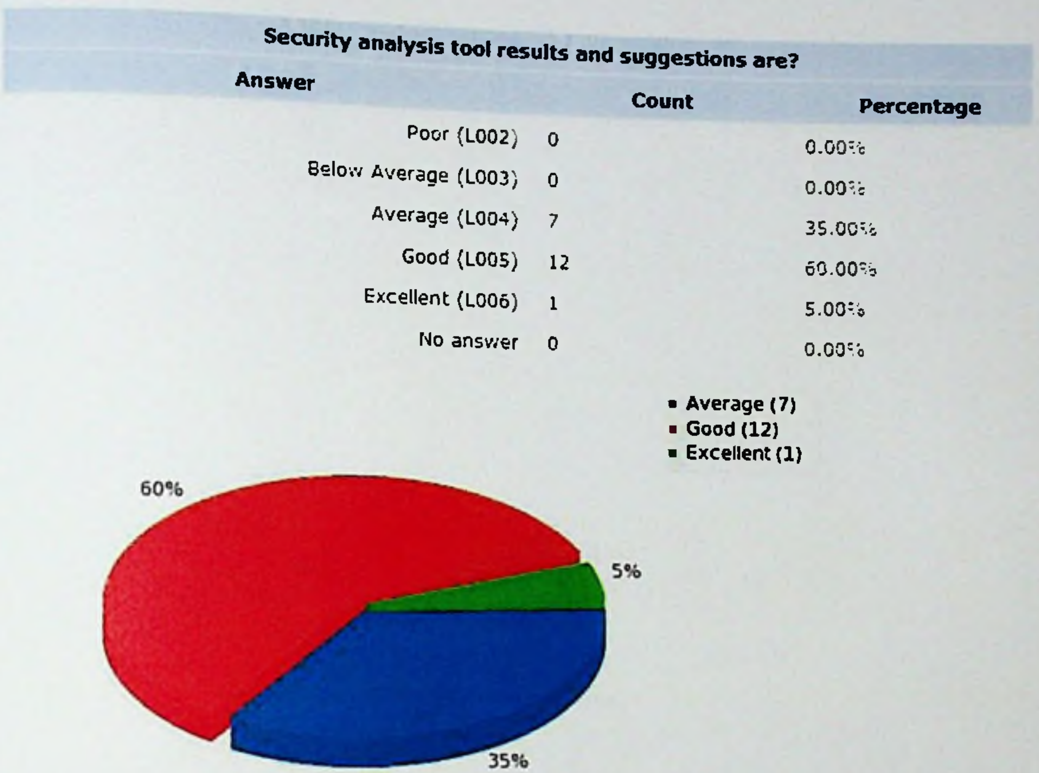
Figure 7-5 : Survey Result Analysis – part 4



How you rank the importance of security analysis modules?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	1	5.00%
Average (L004)	5	25.00%
Good (L005)	10	50.00%
Excellent (L006)	4	20.00%
No answer	0	0.00%

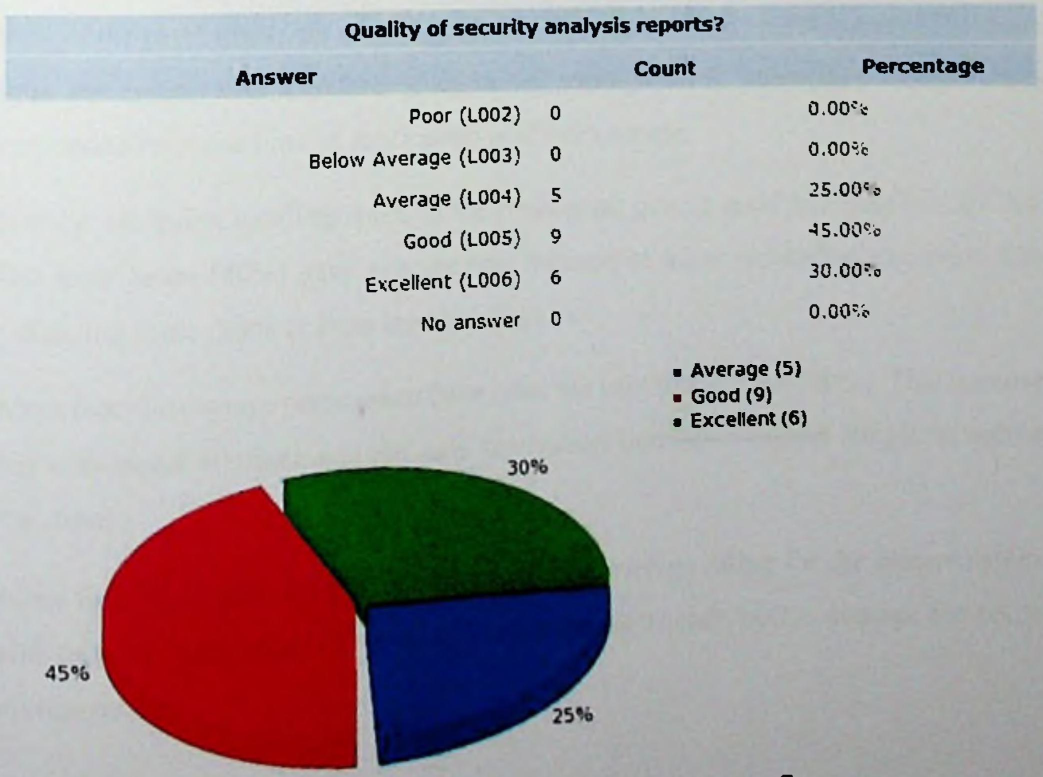
Figure 7-6 : Survey Result Analysis – part 5



Security analysis tool results and suggestions are?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	0	0.00%
Average (L004)	7	35.00%
Good (L005)	12	60.00%
Excellent (L006)	1	5.00%
No answer	0	0.00%

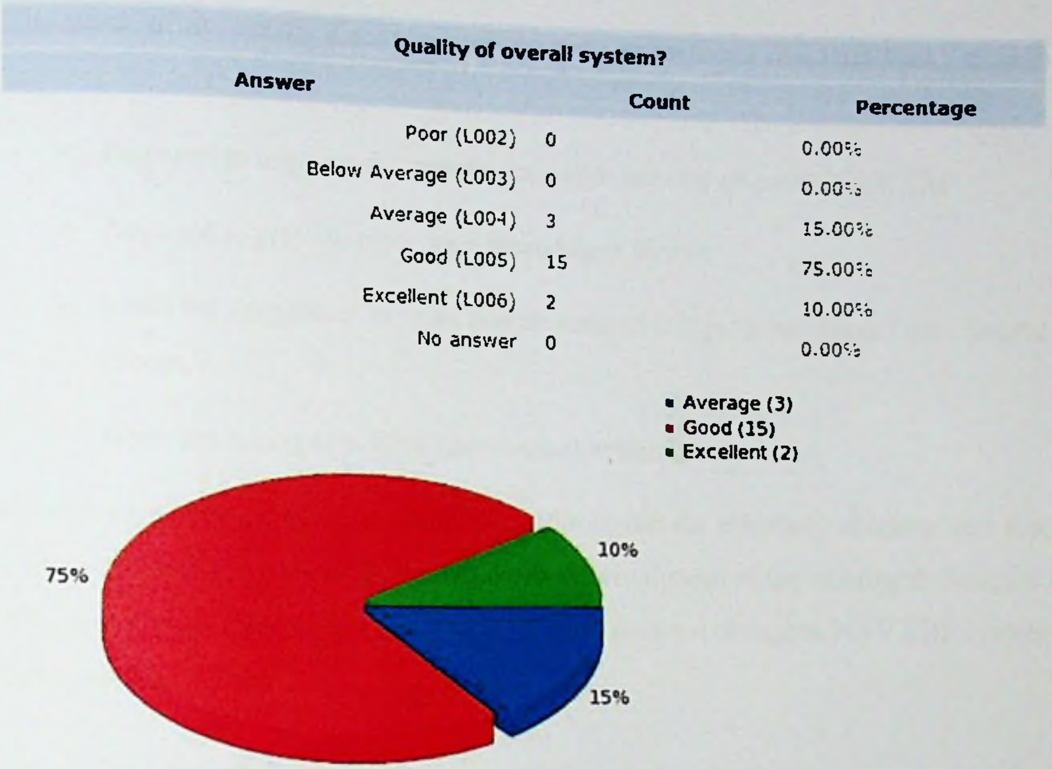
Figure 7-7 : Survey Result Analysis – part 6



Quality of security analysis reports?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	0	0.00%
Average (L004)	5	25.00%
Good (L005)	9	45.00%
Excellent (L006)	6	30.00%
No answer	0	0.00%

Figure 7-8 : Survey Result Analysis – part 7



Quality of overall system?

Answer	Count	Percentage
Poor (L002)	0	0.00%
Below Average (L003)	0	0.00%
Average (L004)	3	15.00%
Good (L005)	15	75.00%
Excellent (L006)	2	10.00%
No answer	0	0.00%

Figure 7-9: Survey Result Analysis – part 8

Here we analysis the survey results by considering the responses for main questions.

95% of the participants are working in the ERP industry. Many participants (85%) have rank the system user interface is above the average level. More than 70% of users responded response time of application is above average.

For the exception handling most of the participant gave a good and excellent (60%). But some users (40%) gave average rate because of some unhandled exception like validating some fields or form inputs may have.

More than the average participants have rated the user friendliness (60%). That because the web based interface and the easy navigation between modules simple to access functions.

More than 65 % participant was rank more than average rating for the system results and security suggestions. Finally, 85% of users have rank above average for entire system quality.

The result of the survey discovers various good suggestions and feed backs to help improve the solution.

- Proposed to improve this solution to cover security of entire NAV ERP.
- Proposed to provide report as a spreadsheet format.
- Some are suggesting to share source code of this program using Open Source license.
- Some are asking to publish user manual within the system.

Overall result has revealed that security auditors can do effective, efficient and fast auditing by using new auditing tools and procedures instead of the existing techniques. The overall objective and scope of a security audit does not change in NAV ERP system environment.

7.4 Summary

This chapter focused on how we evaluate the NAV ERP security analysis tool. Here conducted a questionnaire using an online survey tool for get qualitative attributes. Also after analyzing the survey feedbacks and suggestions we have receive some positive inputs for the future enhancements.

Next chapter, will discuss conclusions and further works of this research project. It will provide an overall achievement, problem encountered, limitations, lesson leant and future works.

Chapter 8

Conclusion and Further works

8.1 Introduction

In the previous chapter it has discussed each and every objective of the solution are make sure that it has been archived.

This is the final chapter of this thesis and presented conclusion and further work of this project. Here explains the overall achievement, problem encountered, limitation, lesson learnt and further work.

8.2 Conclusion

Information security or IT security is the shelter of information itself as well as its information system to make sure CIA; confidentiality, integrity and availability. A number of key roles in organizations are to protect information, to enable the business processes, to provide a protection policy for applications and to protection of technology resources. Therefore, there is a need to ensure a proper security within the organizations internal people or staff, policy and technology components.

8.2.1 Achievements

By reviewing the project from the beginning; we are study the ERP implementation related security issues based on literature survey and the direct observations. After that identified security issues are analysis using the online survey tool. After the requirements analysis survey shows that those identified security issues are significant to the ERP systems security.

System was developed using the most popular LAMP technology and it used many open source tools, libraries and functions to perform its security analysis. The solution take various inputs parameters related to the ERP systems system. Having giving the input system will be analysis the security threats related to ERP systems system. After the analysis phase tool will provide; list of security issues, suggestions for enhance security level of the ERP system, provide list of procedure to follow when using an ERP system and provide automated alert after scanning the ERP system by predefine schedules. This solution can be useful to; ERP systems security auditors, ERP systems system own organizations, ERP systems implementation organizations or anyone who interested to investigate the ERP systems implementation security issues.

Finally evaluating our objectives are put to the questionnaire. By creating the online survey for the target audience (those who are directly associated to the ERP industry). Survey result shows that our solution has recorded 73% of positive performance in the quality, efficiency and accuracy of detection of ERP security issues.

8.2.2 Problem Encountered

At the middle of this research project it was unable to choose better platform to develop our novel solution but analyzing the current available technologies it was identified that using the open source and LAMP stack is suitable for this solution development.

Some audits consume a lot of time and hardware resources; memory, CPU, GPU and disk reads. We are listed how we overcome those problems;

Problem 1: But after choosing the technology it was another problem found that what the best OS to do this solution development?

Solution: By our experience of Linux distribution, we have identified that the Offensive Security Team was producing a penetration testing OS called "Kali Linux" and previously it was named as "Black track Linux".

Problem 2: After that we have few problem; how can we use PHP code to access windows Active directory server for password strength auditing? How can we access Microsoft SQL server database that congaing NAV ERP data?

Solution: By using the self-learning and referencing cited links we have solved those problems and implement our solution.

Problem 3: Auditing AD user's password strength takes lot of time and resources when decrypting the user's password hashes.

Solution: Perform a sequential based audits by splitting hash files into smaller ones.

Speed of Technology Change a Threat to ERP security

Problem 4: Rapid changes of Information Security threats, vulnerabilities, there is no guaranteed our solution will mitigate the identified security issues.

Solution: By observing the latest security threats and vulnerabilities we can update our system to handle those attacking vectors.

8.2.3 Limitations

Few limitations were identified after the evaluation, those are emphasized by the survey participants and by us after the system implementation;

- System must have facility to analyze ERP user wise security threat level.

  When we analyzing security it must be able to track ERP user wise threat level using historical and live data of particular user.

- Enhance the reporting by implementing the export report to spreadsheet.

  All reports must have facility to export as spreadsheet.

- System must cover code level security of NAV ERP.

  It is required to implement a NAV ERP source code level security analysis module to cover security of third party or newly developed modules.

- Integration of user manual to the application.

  Integrating user manual to the system will help to the new users to perform security scanning when by following thee manual.

8.3 Further Works

Previous sections complete the whole research project; however, there are ways to accomplish, improve and confirm this research project understand knowledges. For more studies, few recommendations are discussed in this section.

To cover entire NAV ERP security audit this tool must have to include module to scan NAV ERP source code security. Another one is integrating of the SMS alerting facility when scheduled Cron job found vulnerabilities or security threats. Above mention further works are open for the future researchers.

8.4 Summary

This chapter discusses about conclusion and further works related to this research. The proceeding chapter will contain the list of references that we took the use of when implementing the project.

Reference

[01] Michael E. Whitman and Herbert J. Mattord (2008). Principles of Information Security, Thomson Course Technology

[02] http://www.gartner.com/it-glossary/enterprise-resource-planning-erp/, retrieved on 07th September 2015

[03] http://www.investopedia.com, Retrieved on 07th September 2015

[04] Mohammad A. Rashid (Massey University, New Zealand), Liaquat Hossain (Syracuse University, USA) and Jon David Patrick (University of Sydney, Australia) (2002), The Evolution of ERP Systems: A Historical Perspective

[05] http://www.ehow.com/about_6583617_limitations-erp.html, Retrieved on 07th September 2015

[06] http://www.cvedetails.com/cve/CVE-2010-2083/, Retrieved on 02nd October 2015

[07] http://military.sla.org/nextgov-third-party-software-was-entry-point-for-background-check-system-hack/, Retrieved on 09th October 2015

[08] https://erpscan.com/advisories/erpscan-15-023-sap-afaria-authorization-bypass-insecure-signature/, Retrieved on 03rd January 2016

[09] https://www.htbridge.com/advisory/HTB23245, Retrieved on 05th January 2016

[10] Wei She and Bhavani Thuraisingham (2007), Security for Enterprise Resource Planning Systems

[11] Marnewick, C1 and Labuschagne, L2 (Academy for Information Technology, University of Johannesburg) (2006), A security framework for an ERP system,

[12] David Hendrawirawan, Huseyin Tanriverdi, Carl Zetterlund, Hunaid Hakam, Hyun Ho Kim, Hyewon Paik, CPA, and Yeohoon Yoon., (2007), ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution

[13] http://help.sap.com/r3, Retrieved on 24th January 2016

[14] Ramdas S. Wanare and Amar R. Mudiraj, (2014), Security Issue and their Countermeasures in ERP Implementation

[15] Richardson, B (1998) When Worlds Collide: The Future of ERP and Supply Chain Planning, AMR Research, United States

[16] https://www.turnkeylinux.org/lampstack, Turnkey Linux, Retrieved on 24th January 2016

[17] http://www.opensecurityarchitecture.org/cms/definitions/it-security, IT Security, Retrieved on 24th January 2016

[18] https://www.limesurvey.org/en/about-limesurvey/license, LimeService License and Trademark Guidelines, Retrieved 03rd November 2015

[19] http://mxx.mnstrl.org/, Retrieved 23rd November 2015

[20] http://www.softwareishard.com/blog/firebug/introduction-to-firebug-net-panel/, Retrieved 23rd November 2015

[21] https://blogs.msdn.microsoft.com/developingfordynamicsgp/2008/10/01/ why-does-microsoft-dynamics-gp-encrypt-passwords/, Retrieved on 01st October 2015

[22] Rodi Heijblom (2015), Controlling risks when integrating Mobility and Enterprise Resource Planning (ERP), Master of Business Informatics, Utrecht University

[23] http://www-01.ibm.com/software/analytics/spss/products/statistics/, Retrieved 03rd November 2015

[24] http://www.esri.com/news/arcnews/spring11articles/open-source-technology-and-esri.html, Retrieved 08th December 2015

[25] http://docs.kali.org/introduction/what-is-kali-linux. Retrieved on 08th December 2015

[26] https://www.techopedia.com/definition/4805/virtual-machine-vm, Retrieved on 08th December 2015

[27] http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html, Retrieved on 08th December 2015

[28] http://www.lynda.com/Apache-tutorials/What-Apache-HTTP-Server-what-used-Video/164983/186360-4.html, Retrieved on 08th December 2015

[29] https://www.mysql.com/about/, Retrieved on 08th December 2015

[30] http://php.net/manual/en/intro-whatis.php, Retrieved on 08th December 2015

[31] https://www.phpmyadmin.net/, Retrieved on 08th December 2015

[32] http://www.devdungeon.com/content/how-nmap-scan-php, Retrieved on 16th December 2015

[33] https://blog.joelj.org/windows-password-audit-with-kali-linux/,Retrieved on 9th January 2016

[34] http://tharangac-dynamicsnav.blogspot.com/2014/10/control-add-in-part-01.html/, Retrieved on 10th March 2016

[35] http://bse-c.co.kr/image/3-tier%20architecture.png, Retrieved on 10th March 2016

[36] Shivani Goal, Ravi Kiran, Deepak Garg (2012), Vulnerability Management for an ERP System, International Journal of Computer Application, Vol-53-No.4 Sep-2012, PP 19-22

[37] Christopher, M. and Peck, H (2004), Building Resilient Supply Chain. International Journal of Logistics Management

[38] Sheffi, Y. and Rice, Jr. J. B (2005), A Supply Chain View of the Resilient Enterprise, MIT Sloan Management Review

[39] Rose and Liao, S. (2005), Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. Journal of Regional Science

[40] Fiksel, J (2006), Sustainability and Resilience: Toward a Systems Approach, Sustainability: Science, Practice, & Policy

[41] Wu, B. and Wang, A.D.N (2011), A Multi layer tree model for enterprise vulnerability management. SIGITE'11, (October 20–22), West Point New York USA

[42] Ramdas S. Wanare and Amar R. Mudiraj, (2014), Ramdas S. Wanare and Amar R. Mudiraj, Security Issue and their Countermeasures in ERP Implementation. Dr. Babasaheb Ambedkar Marathwada University, Aurangabad.

[43] Michael E. Whitman and Herbert J. Mattord, (2008), Principles of Information Security, (Kennesaw State University. Kennesaw, Georgia.

Appendixes

Appendix A – NAV ERP system

Figure A - 1 show NAV ERP windows client architecture [34].

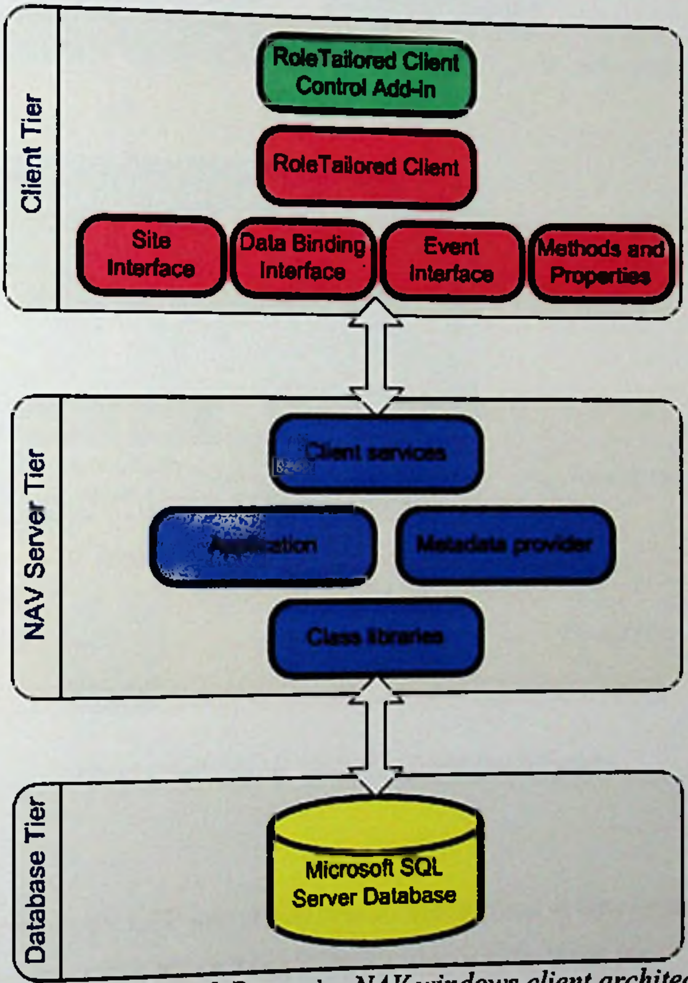


Figure A-1 : Microsoft Dynamics NAV windows client architecture

Figure A - 2 shows NAV ERP three-tier architecture [35].

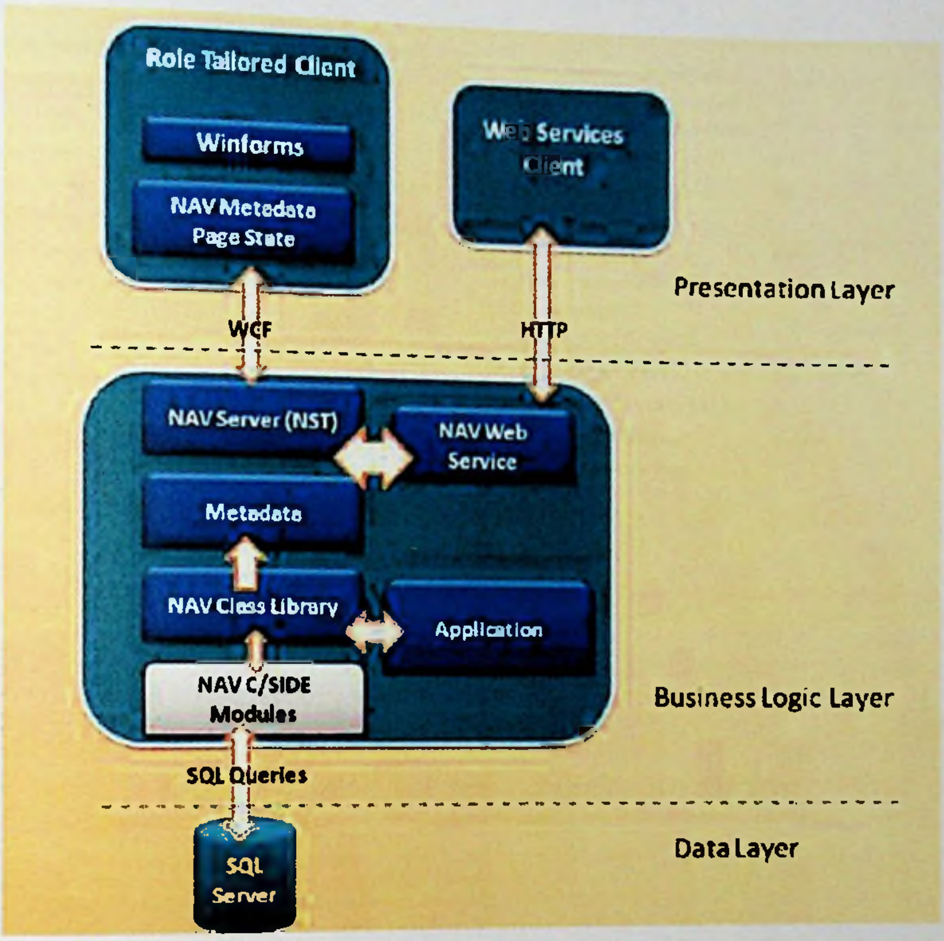
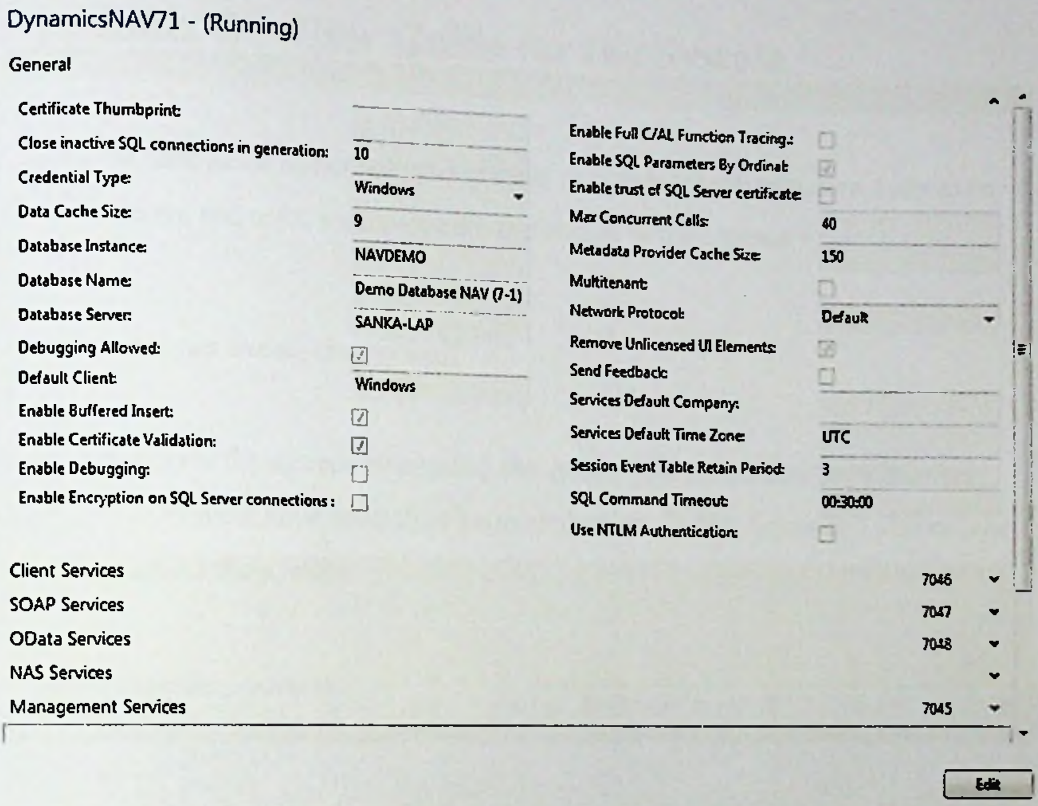


Figure A-2 : NAV ERP three-tier architecture

Figure A-3 shows NAV ERP server configuration interface, it was located on the ERP server computers program file -> NAV ERP administration tool path.



DynamicsNAV71 - (Running)

General

Certificate Thumbprint:

Close inactive SQL connections in generation: 10

Credential Type: Windows

Data Cache Size: 9

Database Instance: NAVDEMO

Database Name: Demo Database NAV (7-1)

Database Server: SANKA-LAP

Debugging Allowed: ☑

Default Client: Windows

Enable Buffered Insert: ☑

Enable Certificate Validation: ☑

Enable Debugging: □

Enable Encryption on SQL Server connections : □

Enable Full C/AL Function Tracing: □

Enable SQL Parameters By Ordinal: ☑

Enable trust of SQL Server certificate: □

Max Concurrent Calls: 40

Metadata Provider Cache Size: 150

Multitenant: □

Network Protocol: Default

Remove Unlicensed UI Elements: ☑

Send Feedback: □

Services Default Company:

Services Default Time Zone: UTC

Session Event Table Retain Period: 3

SQL Command Timeout: 00:30:00

Use NTLM Authentication: □

Client Services 7046

SOAP Services 7047

OData Services 7048

NAS Services

Management Services 7045

Figure A-3 : NAV ERP server configuration interface

Appendix B – User Guide for the System

This is the user guide of our solution in order to running the application users must have hardware and software that we are mentioned in the Chapter 1.

B.1 How we can access the system?

Users can access the system by entering the system address on their web browser. After that they must have enter their login credentials. Below figure B-1 shows how users can access the system.

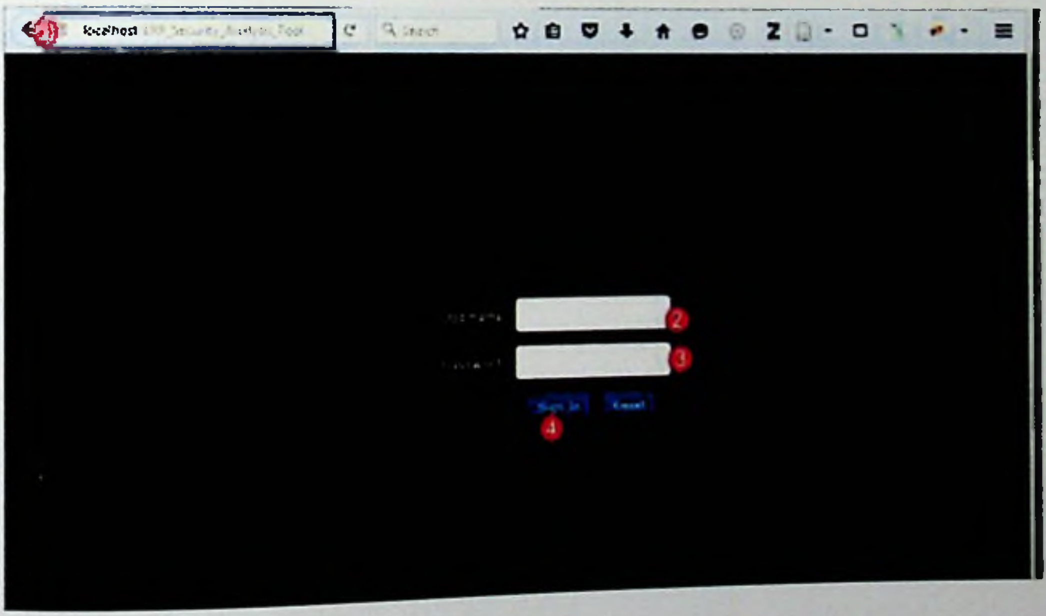


Figure B-1 : System login screen

After successful login users can view there dashboard to perform various function that we have implemented within the system.

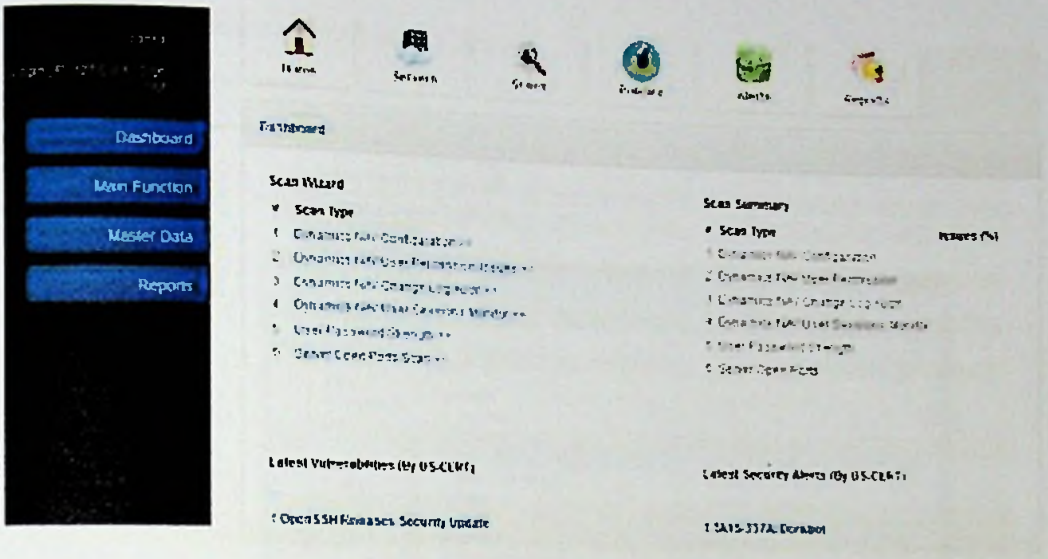

Dashboard
Main Function
Master Data
Reports
Dashboard
Scan Wizard
Scan Type
Scan Summary
Scan Type
Issues (%)
Latest Vulnerabilities (By US-CERT)
Latest Security Alerts (By US-CERT)
OpenSSH Releases Security Update

Figure B-2 : System dashboard

According to the user requirement they can perform actions within the system by clicking on the hyperlink, main system icons or navigating through the menu bar. Below sub sections we describe how to perform system main security scanning's and audits.

B.2 How do we scan NAV ERP server configuration?

To perform a NAV ERP server security scan user must have permission to read "*CustomSettings.config*" file that was located inside the NAV ERP server installation folder (Ex: *Program Files\Microsoft Dynamics NAV\71\Service*).

Step 01: Click on the "Dynamics NAV Configuration" link, it will open server configuration scan main page that consist of all scan data.

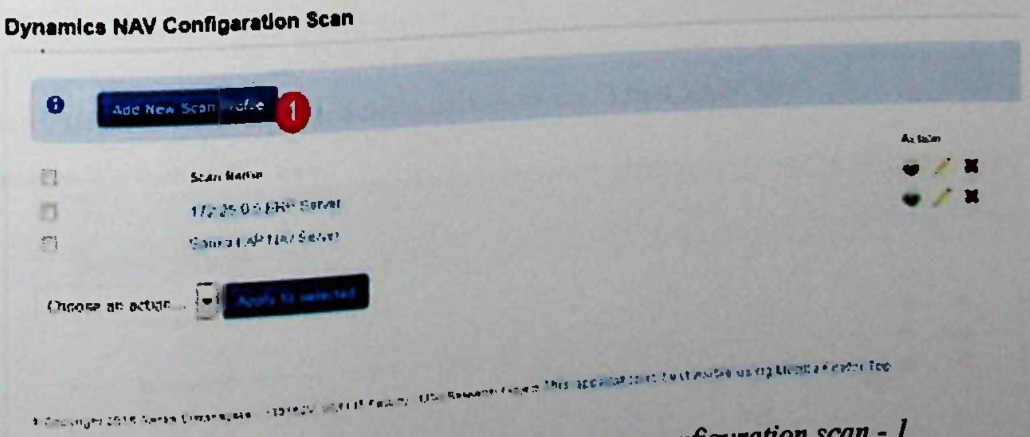
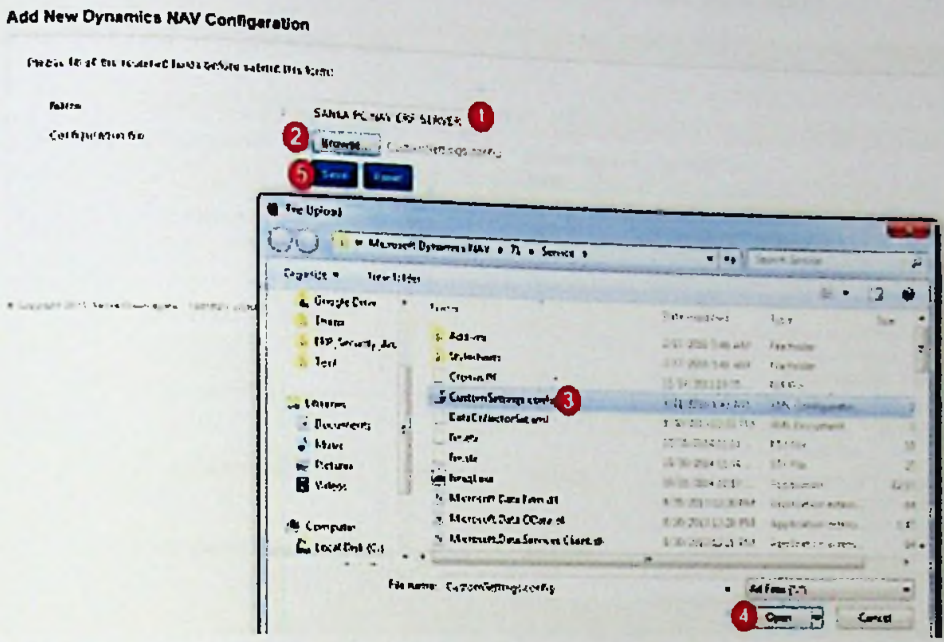


Figure B-3 : Performing a NAV ERP Server configuration scan - 1

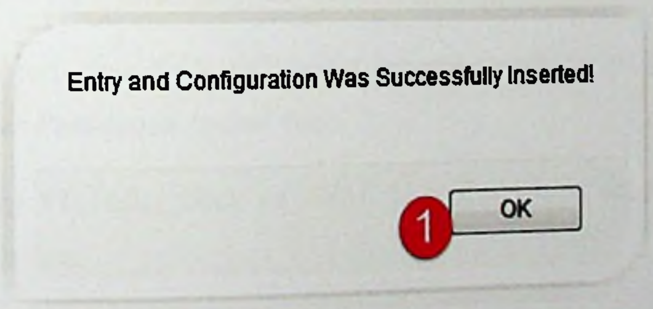
Step 02: Click on add new scan profile button.



Add New Dynamics NAV Configaration

Figure B-4 : Uploading NAV ERP configuration file

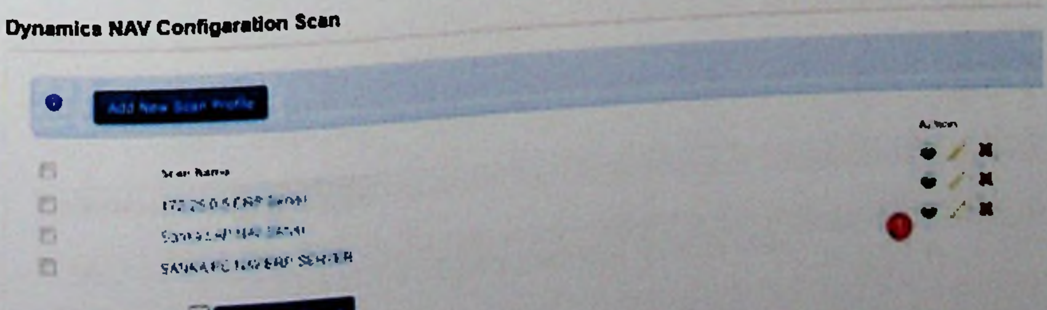
Step 03: After entering all form data click on save button.



Entry and Configuration Was Successfully Inserted!

Figure B-5 : Upload confirm dialog

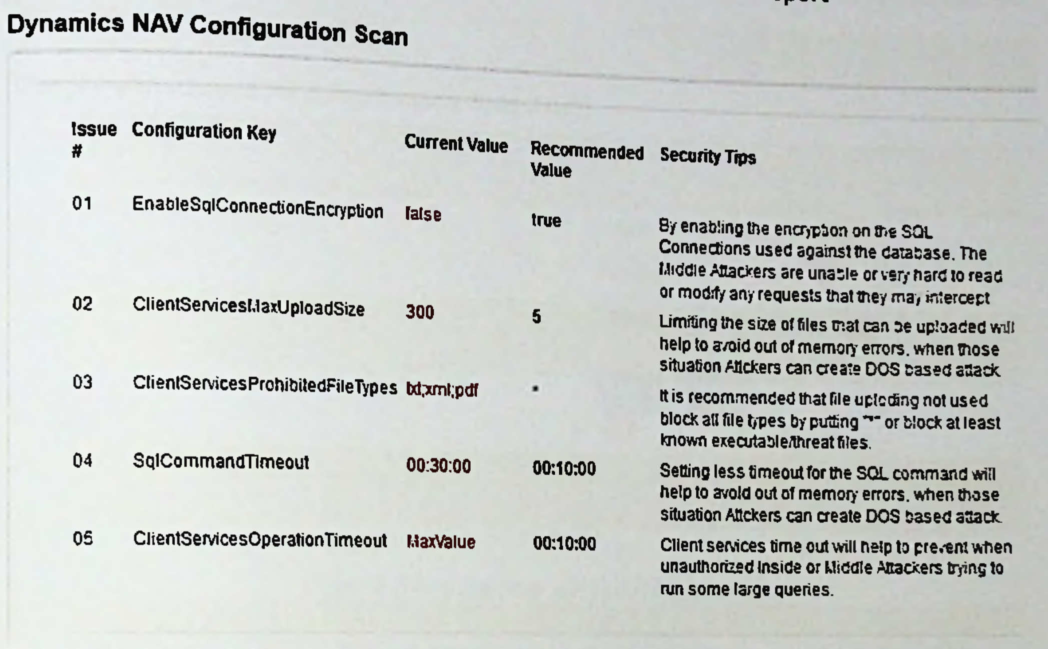
Step 04: Performing a security scan by clicking on the "1 (red color)" icon



Dynamica NAV Configaration Scan

Figure B-6 : Perform a security scan

Step 05: After the clicking on scan icon system will display the Scan report



Dynamics NAV Configuration Scan

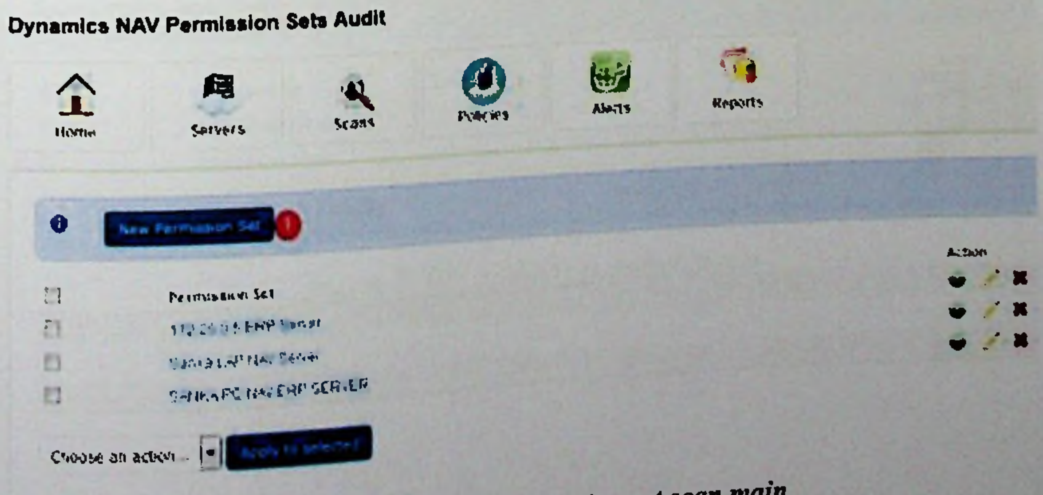
Issue #	Configuration Key	Current Value	Recommended Value	Security Tips
01	EnableSqlConnectionEncryption	false	true	By enabling the encryption on the SQL Connections used against the database. The Middle Attackers are unable or very hard to read or modify any requests that they may intercept
02	ClientServicesMaxUploadSize	300	5	Limiting the size of files that can be uploaded will help to avoid out of memory errors. when those situation Atickers can create DOS based attack
03	ClientServicesProhibitedFileTypes	txt;xml;pdf	*	It is recommended that file uplcding not used block all file types by putting "*" or block at least known executable/threat files.
04	SqlCommandTimeout	00:30:00	00:10:00	Setting less timeout for the SQL command will help to avoid out of memory errors. when those situation Atickers can create DOS based attack
05	ClientServicesOperationTimeout	MaxValue	00:10:00	Client services time out will help to prevent when unauthorized inside or Middle Attackers trying to run some large queries.

Figure B-7 : Scan summary report

B.3 How do we scan NAV ERP User Permission Issues?

To perform a NAV ERP server permission issue scan, users must click on the "*NAV User Permission Issues*" link.

Step 01: After click on "*NAV User Permission Issues*" link you will see below interface;



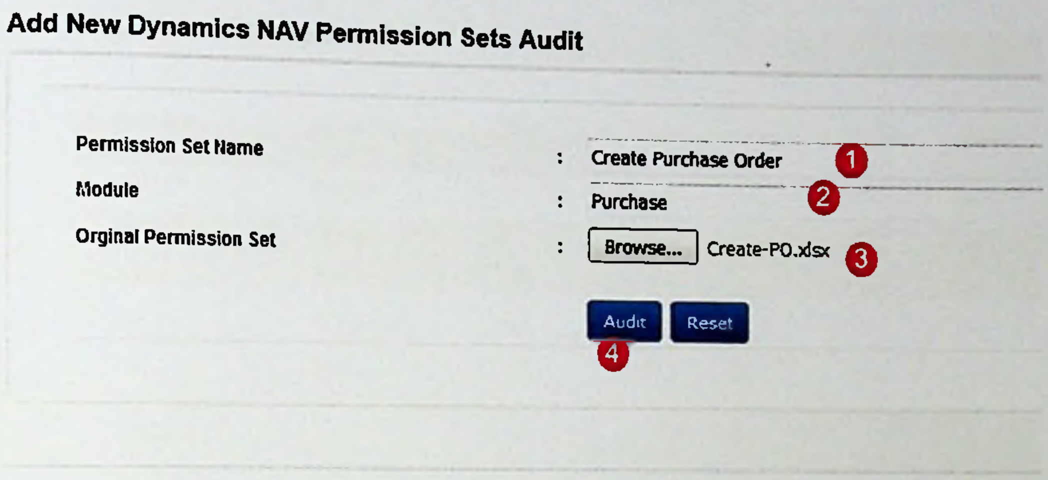
Dynamics NAV Permission Sets Audit

	Permission Set
□	[illegible] ERP Server
□	[illegible] NAV Server
□	[illegible] NAV ERP SERVER

Choose an action... ▾ Apply to selected

Figure B-8 : User permission set scan main

Step 02: To add new permission set you must need to click on "New Permission Set" link.


Add New Dynamics NAV Permission Sets Audit

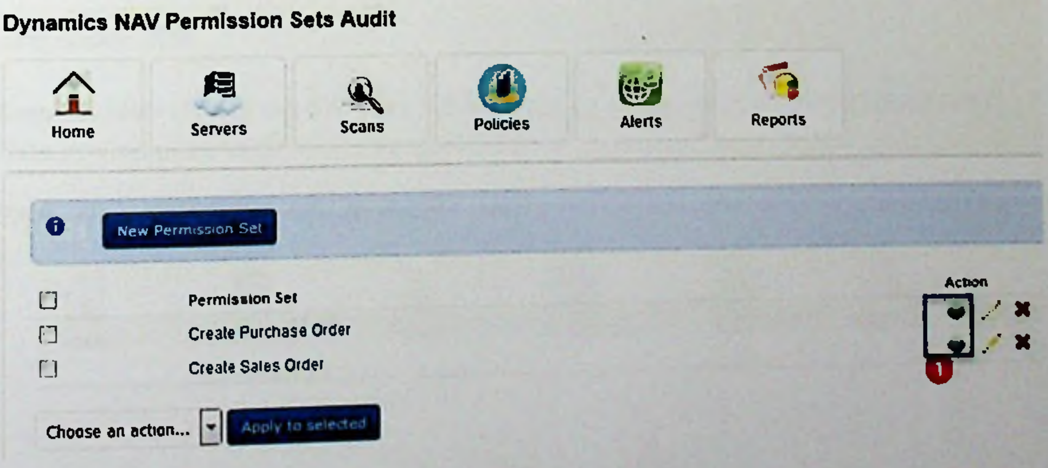
Permission Set Name : Create Purchase Order

Module : Purchase

Orginal Permission Set : Browse... Create-PO.xlsx

Figure B-9 : Adding new permission set

Step 03: After uploading main permission sets users can audit permission set by comparing the live NAV ERP server permission set.


Dynamics NAV Permission Sets Audit

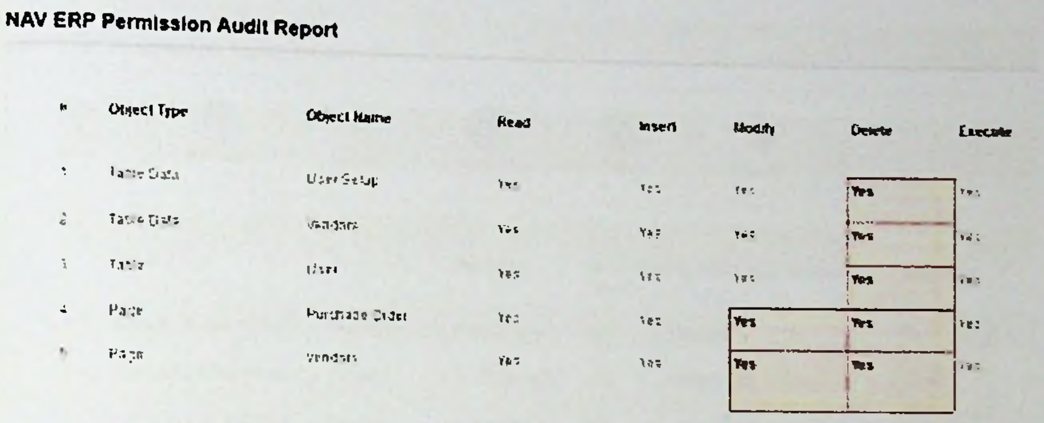
□ Permission Set

□ Create Purchase Order

□ Create Sales Order

Figure B-10 : Auditing permission sets

Step 04: After the auditing phase if system found permission conflicts then users will see report that containing those conflict entries.



NAV ERP Permission Audit Report

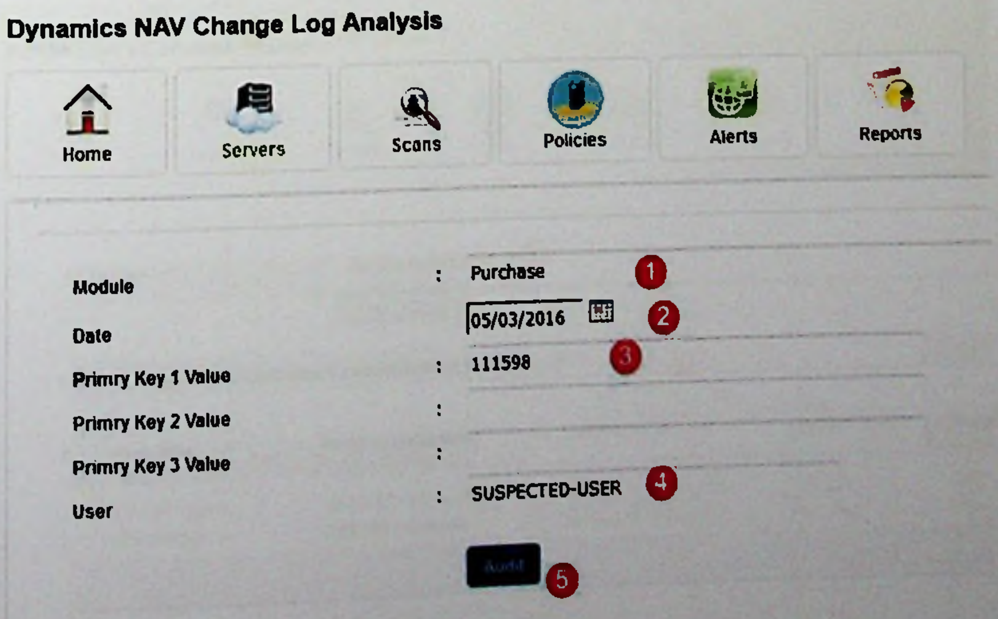
#	Object Type	Object Name	Read	Insert	Modify	Delete	Execute
1	Table Data	User Setup	Yes	Yes	Yes	Yes	Yes
2	Table Data	Vendors	Yes	Yes	Yes	Yes	Yes
3	Table	Users	Yes	Yes	Yes	Yes	Yes
4	Page	Purchase Order	Yes	Yes	Yes	Yes	Yes
5	Page	Vendors	Yes	Yes	Yes	Yes	Yes

Figure B-11 : Permission conflict entries report

B.4 how do we audit NAV change log issues?

To perform a NAV ERP change log issue scan users must click on the "*NAV Change Log Audit*" link.

Step 01: After clicking the link users will see audit data filtering form by entering relevant data user required to click on Audit button (5)

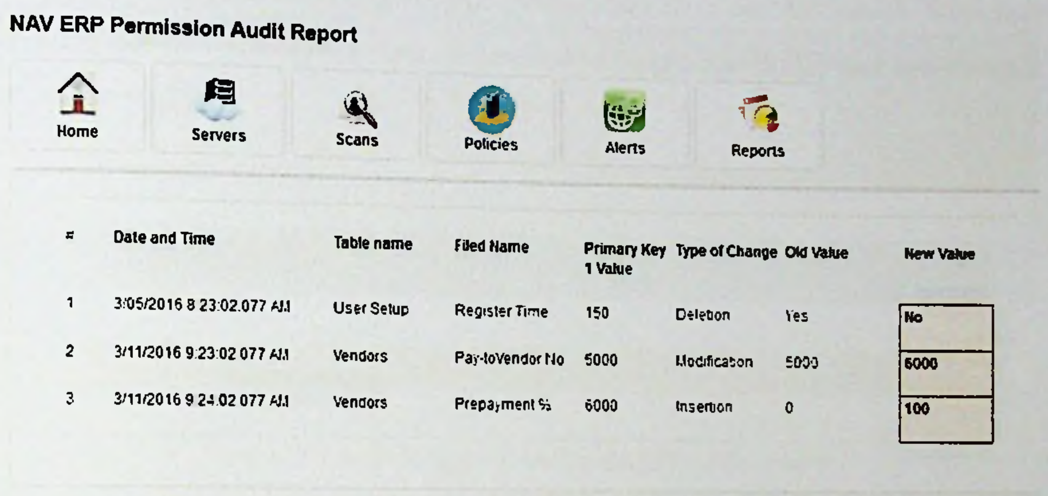


Dynamics NAV Change Log Analysis

Module	:	Purchase
Date		05/03/2016
Primry Key 1 Value	:	111598
Primry Key 2 Value	:	
Primry Key 3 Value	:	
User	:	SUSPECTED-USER

Figure B-12 : Change log audit form

Step 02: If system found results based on user entered values system will display a list of changes as follows;



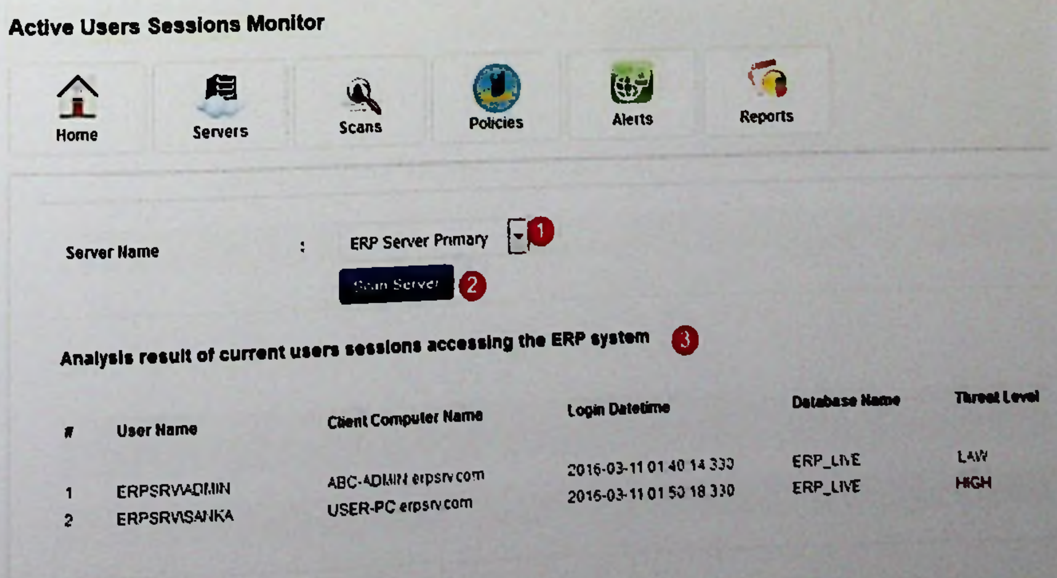
NAV ERP Permission Audit Report

#	Date and Time	Table name	Filed Name	Primary Key 1 Value	Type of Change	Old Value	New Value
1	3/05/2016 8 23:02.077 AM	User Setup	Register Time	150	Deletion	Yes	No
2	3/11/2016 9:23:02 077 AM	Vendors	Pay-toVendor No	5000	Modification	5000	6000
3	3/11/2016 9 24.02 077 AM	Vendors	Prepayment %	6000	Insertion	0	100

Figure B-13 : Change log audit report

B.5 How do we monitor NAV user sessions?

To view the NAV ERP user session report they users must need to click on the "*NAV User Sessions Monitor*" link. After clicking link figure B – 15 form will display by selecting relevant server using the drop down menu users can view user session report.



Active Users Sessions Monitor

Server Name : ERP Server Primary

Analysis result of current users sessions accessing the ERP system

#	User Name	Client Computer Name	Login Datetime	Database Name	Threat Level
1	ERPSRV\ADMIN	ABC-ADMIN erpsrv.com	2016-03-11 01 40 14 330	ERP_LIVE	LAW
2	ERPSRV\SANKA	USER-PC erpsrv.com	2016-03-11 01 50 18 330	ERP_LIVE	HIGH

Figure B-14 : User session monitoring report

B. 6 How do we audit NAV ERP user's password strength?

Step 01: Users required obtain NTDIS database file from the AD server. After that clicking add new scan profile link on password strength master file user can create a new scan profile.

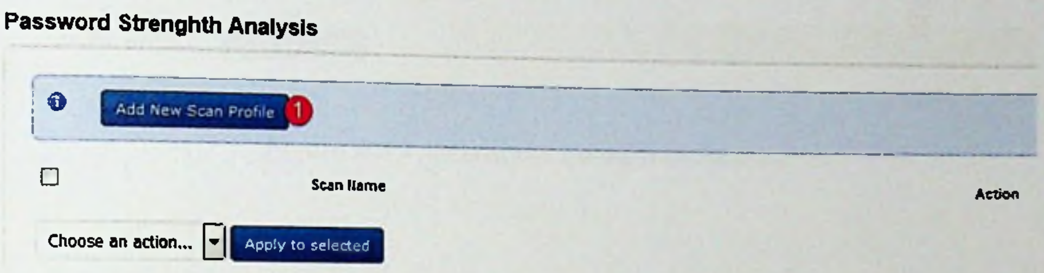
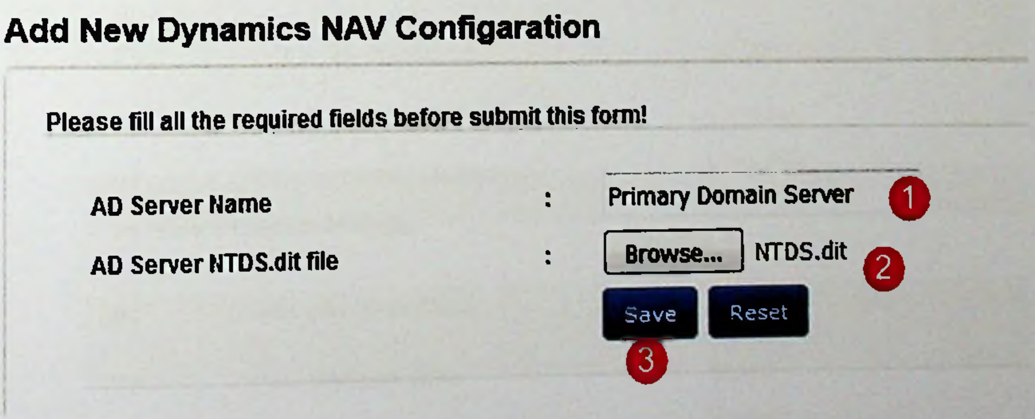


Figure B-15 : Password strength audit profile create 1

Step 02: Using the data upload form users can create new scan profile with relevant NTDIS database file.



Add New Dynamics NAV Configaration

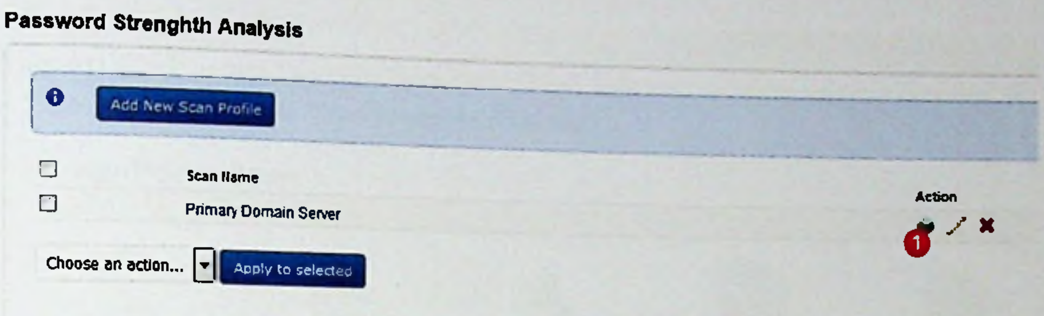
Please fill all the required fields before submit this form!

AD Server Name : Primary Domain Server

AD Server NTDS.dit file : NTDS.dit

Figure B-16 : Password strength audit profile create 2

Step 03: By clicking relevant server profile scan button users can perform audits.



Password Strenghth Analysis

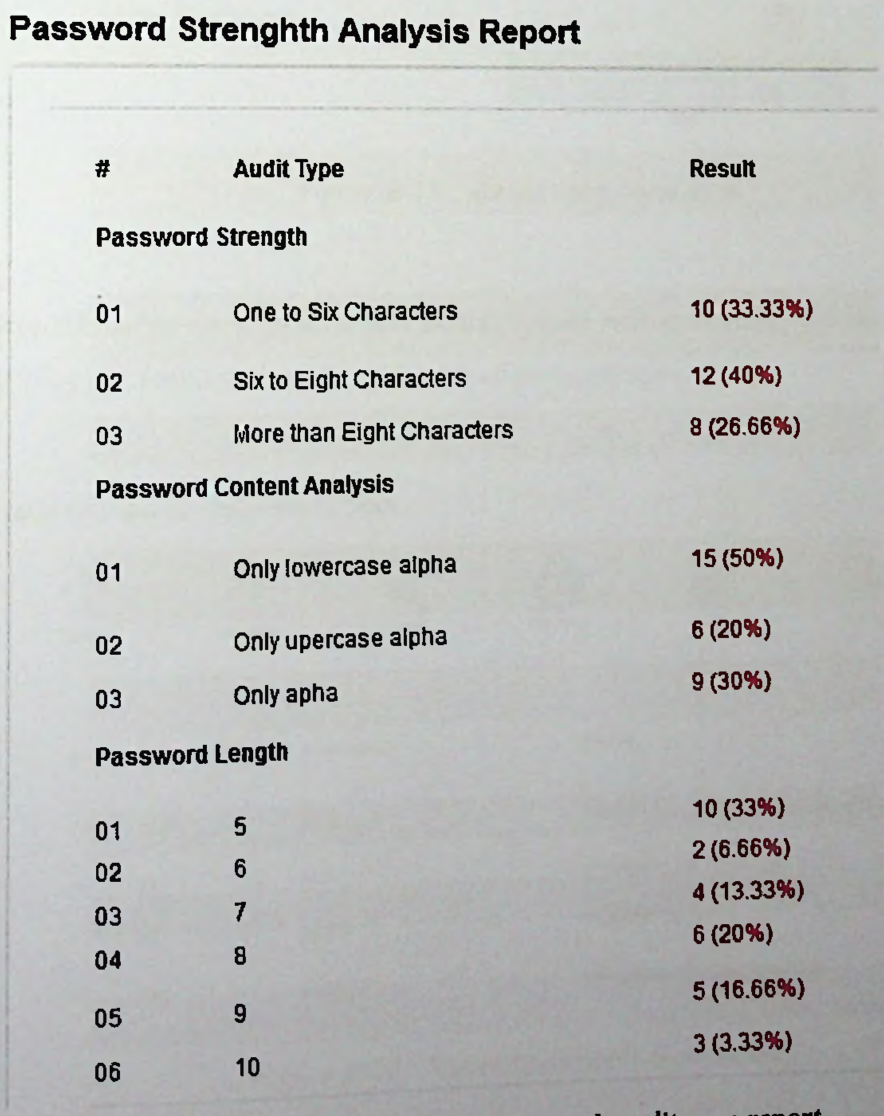
Add New Scan Profile

	Scan Name	Action
□	Primary Domain Server	

Choose an action... ▾ Apply to selected

Figure B-17 : Password strength audit scan

Step 04: View password strength report details.



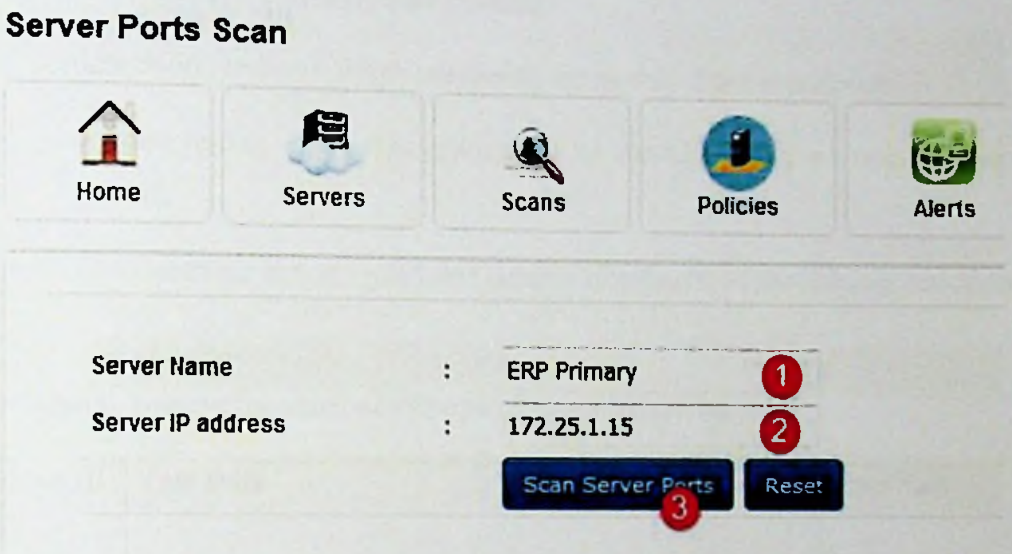
Password Strenghth Analysis Report

#	Audit Type	Result
Password Strength		
01	One to Six Characters	10 (33.33%)
02	Six to Eight Characters	12 (40%)
03	More than Eight Characters	8 (26.66%)
Password Content Analysis		
01	Only lowercase alpha	15 (50%)
02	Only upercase alpha	6 (20%)
03	Only apha	9 (30%)
Password Length		
01	5	10 (33%)
02	6	2 (6.66%)
03	7	4 (13.33%)
04	8	6 (20%)
05	9	5 (16.66%)
06	10	3 (3.33%)

Figure B-18: Password strength audit scan report

B.7 How do we scan NAV ERP server open ports?

Step 01: Click on the "*Server Open Ports Scan*" link and entering server name and IP address. After that click *"Scan Server Port"* button.

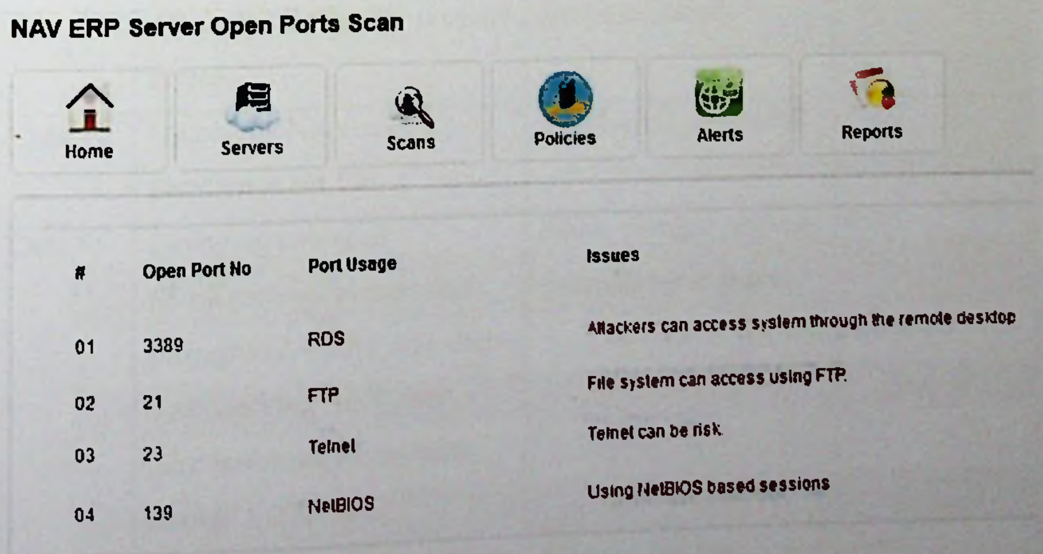


Server Name : ERP Primary

Server IP address : 172.25.1.15

Figure B-19 : Server open ports scan

Step 02: After click on scan port button system will scan server for open ports and display if it found vulnerable or risk based ports are open



#	Open Port No	Port Usage	Issues
01	3389	RDS	Attackers can access system through the remote desktop
02	21	FTP	File system can access using FTP.
03	23	Telnet	Telnet can be risk.
04	139	NetBIOS	Using NetBIOS based sessions

Figure B-20 : Server open ports scan report

Appendix C – Test cases and test results

System has been tested using standard software testing process;

1. Unit testing – Test individual modules
2. Integration testing – When integrating the module this test performs.
3. System testing – After integrating the all module finally we test the entire system.
4. User interface testing – confirms the user interface have the industry standards.

In Table C-1 shows the detail description of the test cases and result.

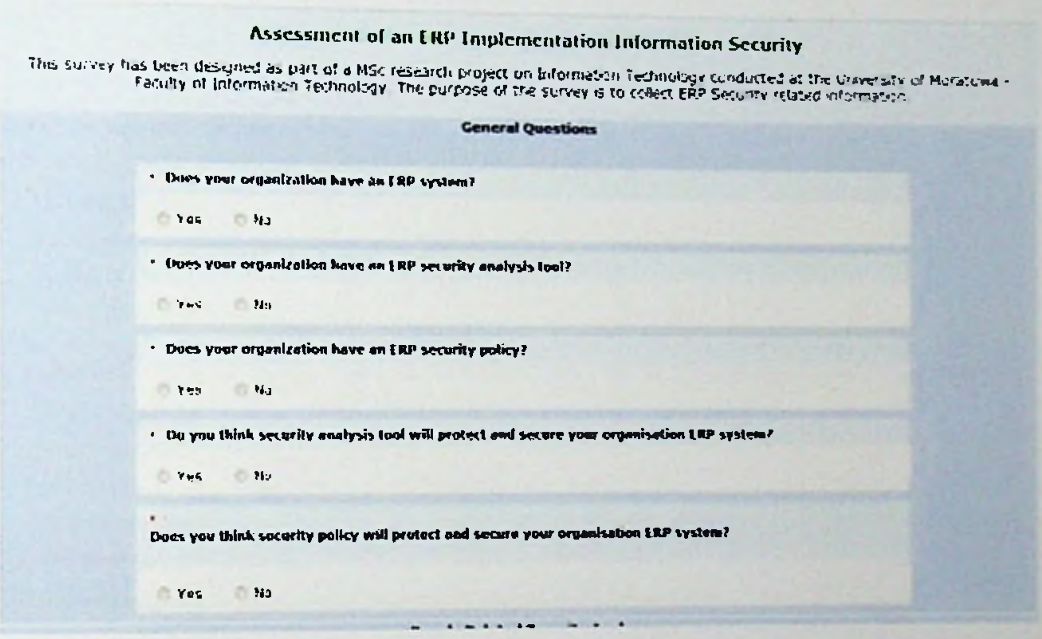
Case ID	Test Data	Expected Results	Pass/Fail
Case 1	Upload the NAV ERP server configuration file	Successfully uploaded	Pass
Case 2	Scan NAV ERP configuration data having security issues	found security issues are shown report with suggestions	Pass
Case 3	Scan NAV ERP configuration data after fixing the security issues	Show report indicating no issues found.	Pass
Case 4	Uploading NAV user permission set file	Successfully uploaded	Pass
Case 5	Changing uploaded permission set related data through NAV ERP and after that checking NAV user permission set for security issues	Show changed security permissions as report.	Pass
Case 6	Create new vendor and delete that vendor after that audit Vendor id and deleted user	Show deleted user related change log data	Pass

	name using NAV change log audit form.		
Case 7	Login to the system and change logged on computers name as “XYZ-PC” then restart computer and logon to the system. After that check NAV ERP user session audit report.	Show changed pc name and logon users name as conflict session.	Pass
Case 8	In the windows domain controller create 10 users with same password and same character length, after that run the password strength scan	Show newly created user’s password strength data by updating existing contain user’s data as a report.	Pass
Case 9	ERP server computer create firewall rule to allow remote desktop, after that analysis server open port.	Report display port 3389 is open.	Pass
Case 10	Access the system by giving a wrong credential	Show error message saying user name or password incorrect	Pass

Table C-1 : Test cases and test results

Appendix D – Questionnaire used for requirement analysis

We have conducted an online survey using the "*LimeSurvey*" for the analysis of security issues founded during the literature review.



Assessment of an ERP Implementation Information Security

This survey has been designed as part of a MSc research project on Information Technology conducted at the University of Moratuwa - Faculty of Information Technology. The purpose of the survey is to collect ERP Security related information.

General Questions

- **Does your organization have an ERP system?**

○ Yes ○ No

- **Does your organization have an ERP security analysis tool?**

○ Yes ○ No

- **Does your organization have an ERP security policy?**

○ Yes ○ No

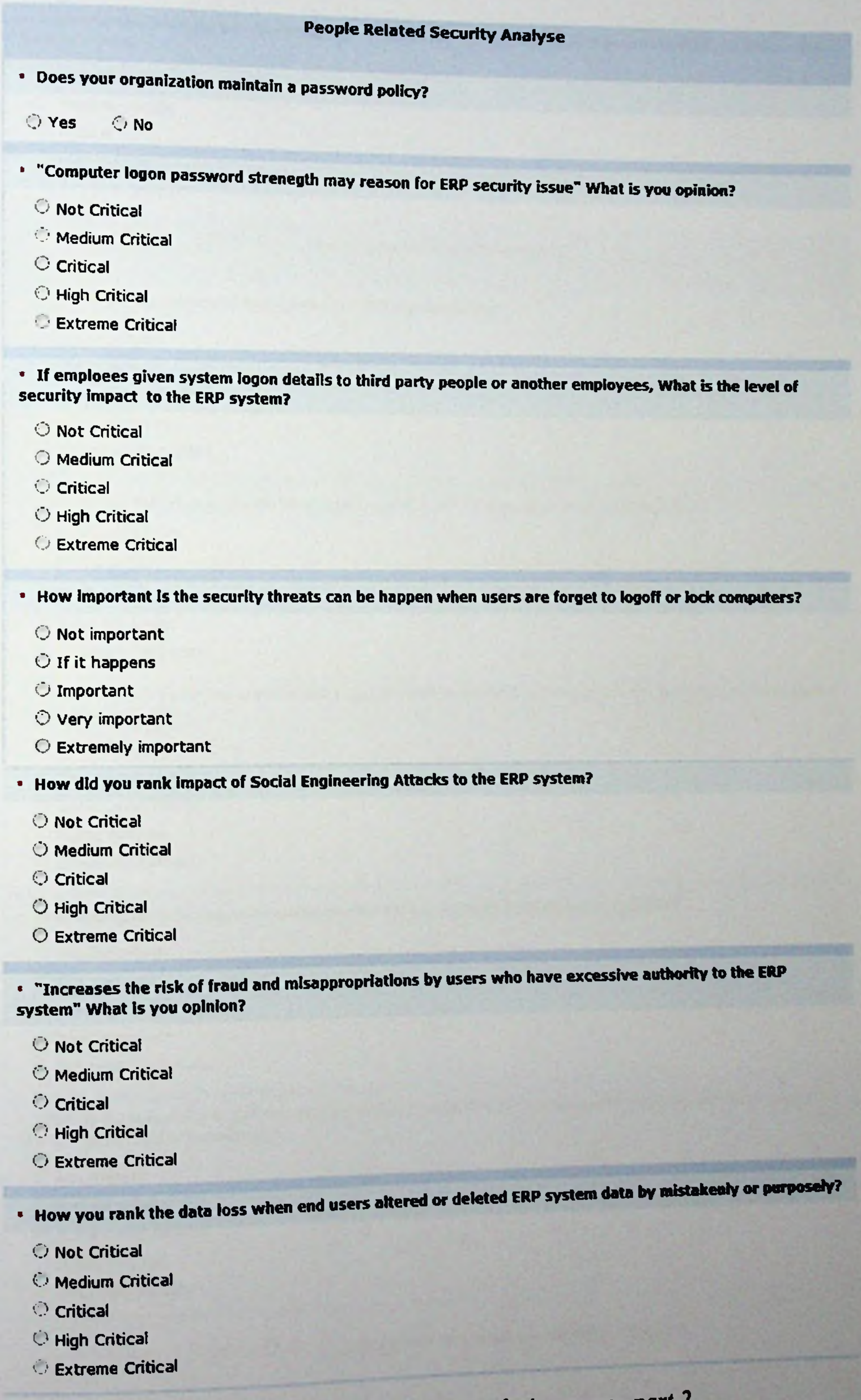
- **Do you think security analysis tool will protect and secure your organisation ERP system?**

○ Yes ○ No

- **Does you think security policy will protect and secure your organisation ERP system?**

○ Yes ○ No

Figure D-1 : Requirements analysis survey - part 1



People Related Security Analyse

- Does your organization maintain a password policy?

○ Yes ○ No

- "Computer logon password strenegth may reason for ERP security issue" What is you opinion?

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

- If emploees given system logon details to third party people or another employees, What is the level of security impact to the ERP system?

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

- How important is the security threats can be happen when users are forget to logoff or lock computers?

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

- How did you rank impact of Social Engineering Attacks to the ERP system?

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

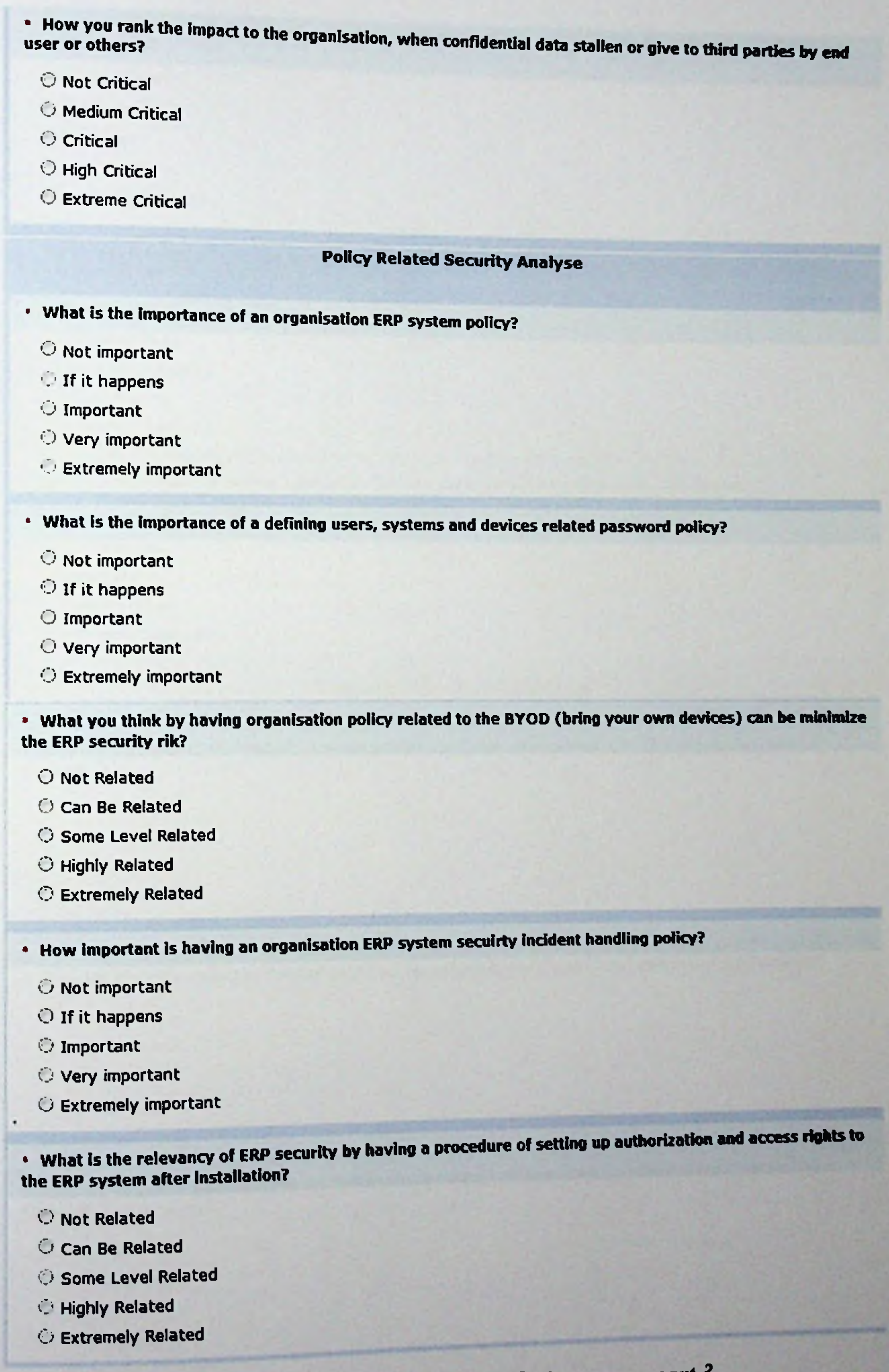
- "Increases the risk of fraud and misappropriations by users who have excessive authority to the ERP system" What is you opinion?

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

- How you rank the data loss when end users altered or deleted ERP system data by mistakealy or purposely?

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

Figure D-2 : Requirements analysis survey - part 2



- How you rank the impact to the organisation, when confidential data stallen or give to third parties by end user or others?

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

Policy Related Security Analyse

- What is the importance of an organisation ERP system policy?

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

- What is the importance of a defining users, systems and devices related password policy?

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

- What you think by having organisation policy related to the BYOD (bring your own devices) can be minimize the ERP security rik?

○ Not Related
○ Can Be Related
○ Some Level Related
○ Highly Related
○ Extremely Related

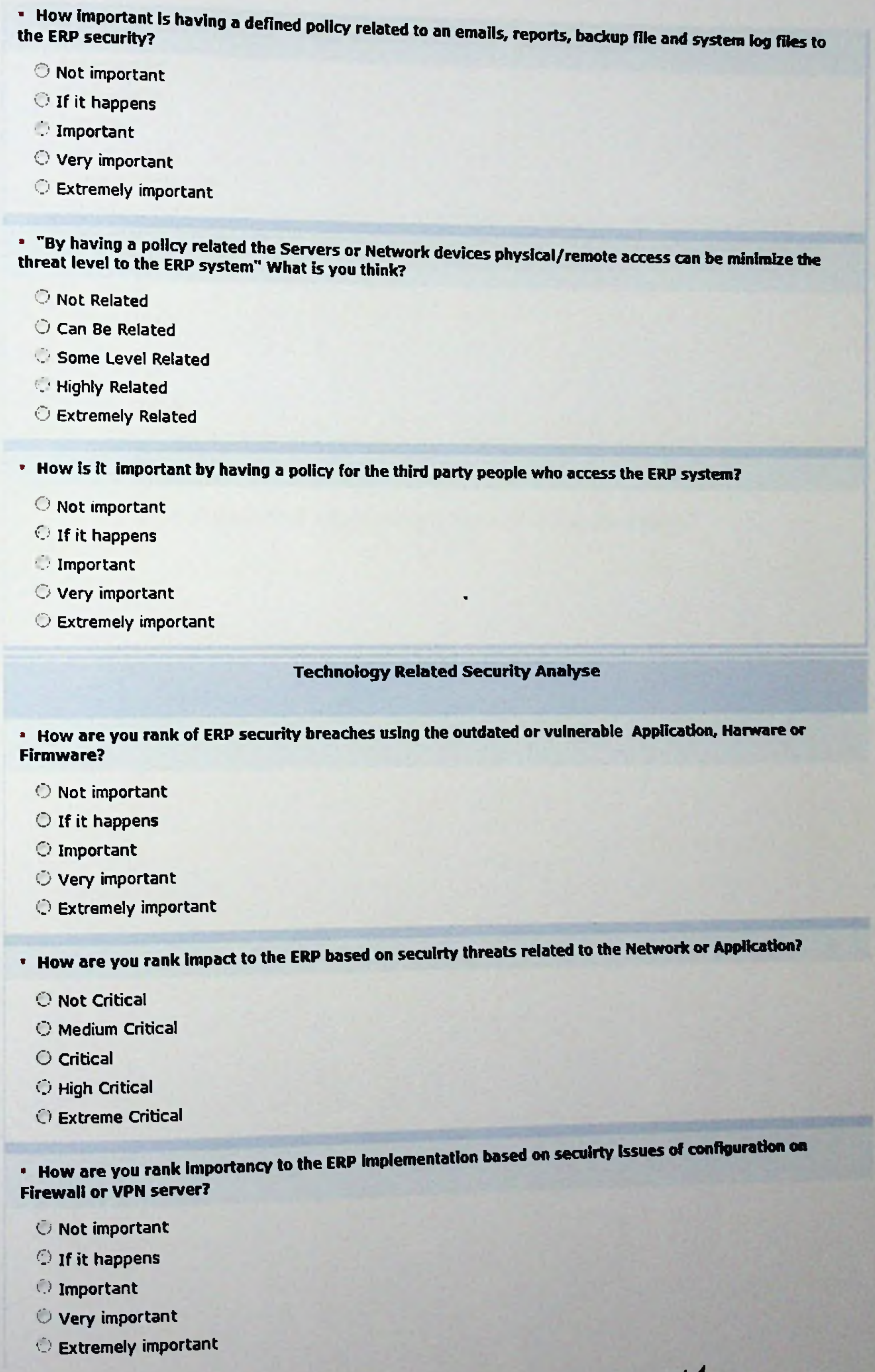
- How important is having an organisation ERP system secuirty incident handling policy?

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

- What is the relevancy of ERP security by having a procedure of setting up authorization and access rights to the ERP system after installation?

○ Not Related
○ Can Be Related
○ Some Level Related
○ Highly Related
○ Extremely Related

Figure D-3 : Requirements analysis survey - part 3



- **How important is having a defined policy related to an emails, reports, backup file and system log files to the ERP security?**

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

- **"By having a policy related the Servers or Network devices physical/remote access can be minimize the threat level to the ERP system" What is you think?**

○ Not Related
○ Can Be Related
○ Some Level Related
○ Highly Related
○ Extremely Related

- **How is it important by having a policy for the third party people who access the ERP system?**

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

Technology Related Security Analyse

- **How are you rank of ERP security breaches using the outdated or vulnerable Application, Harware or Firmware?**

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

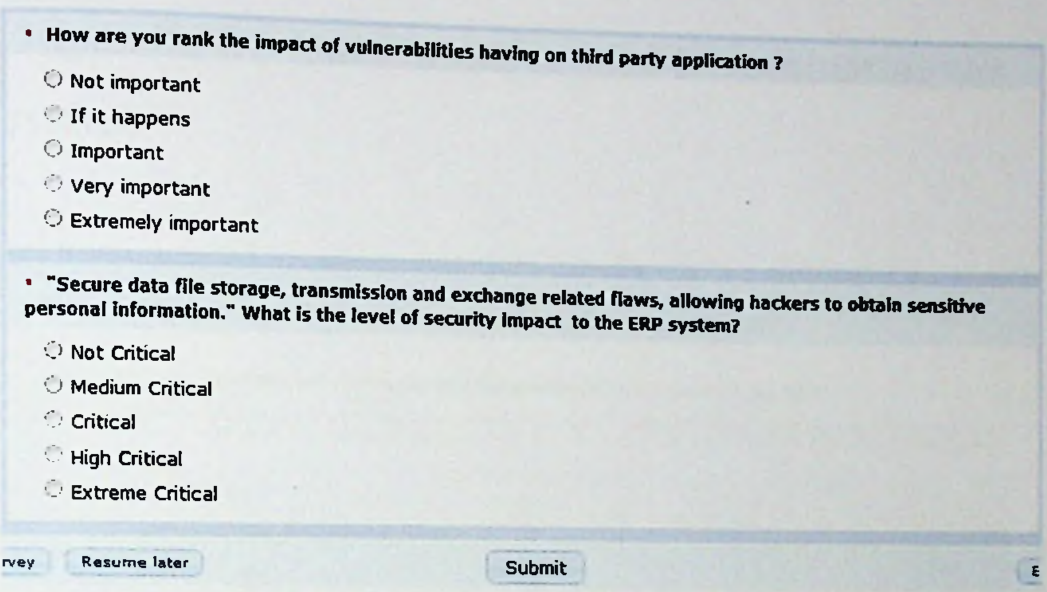
- **How are you rank impact to the ERP based on seculrty threats related to the Network or Application?**

○ Not Critical
○ Medium Critical
○ Critical
○ High Critical
○ Extreme Critical

- **How are you rank importancy to the ERP implementation based on seculrty issues of configuration on Firewall or VPN server?**

○ Not important
○ If it happens
○ Important
○ Very important
○ Extremely important

Figure D-4 : Requirements analysis survey - part 4



- How are you rank the impact of vulnerabilities having on third party application ?

○ Not important

○ If it happens

○ Important

○ Very important

○ Extremely important

- "Secure data file storage, transmission and exchange related flaws, allowing hackers to obtain sensitive personal information." What is the level of security impact to the ERP system?

○ Not Critical

○ Medium Critical

○ Critical

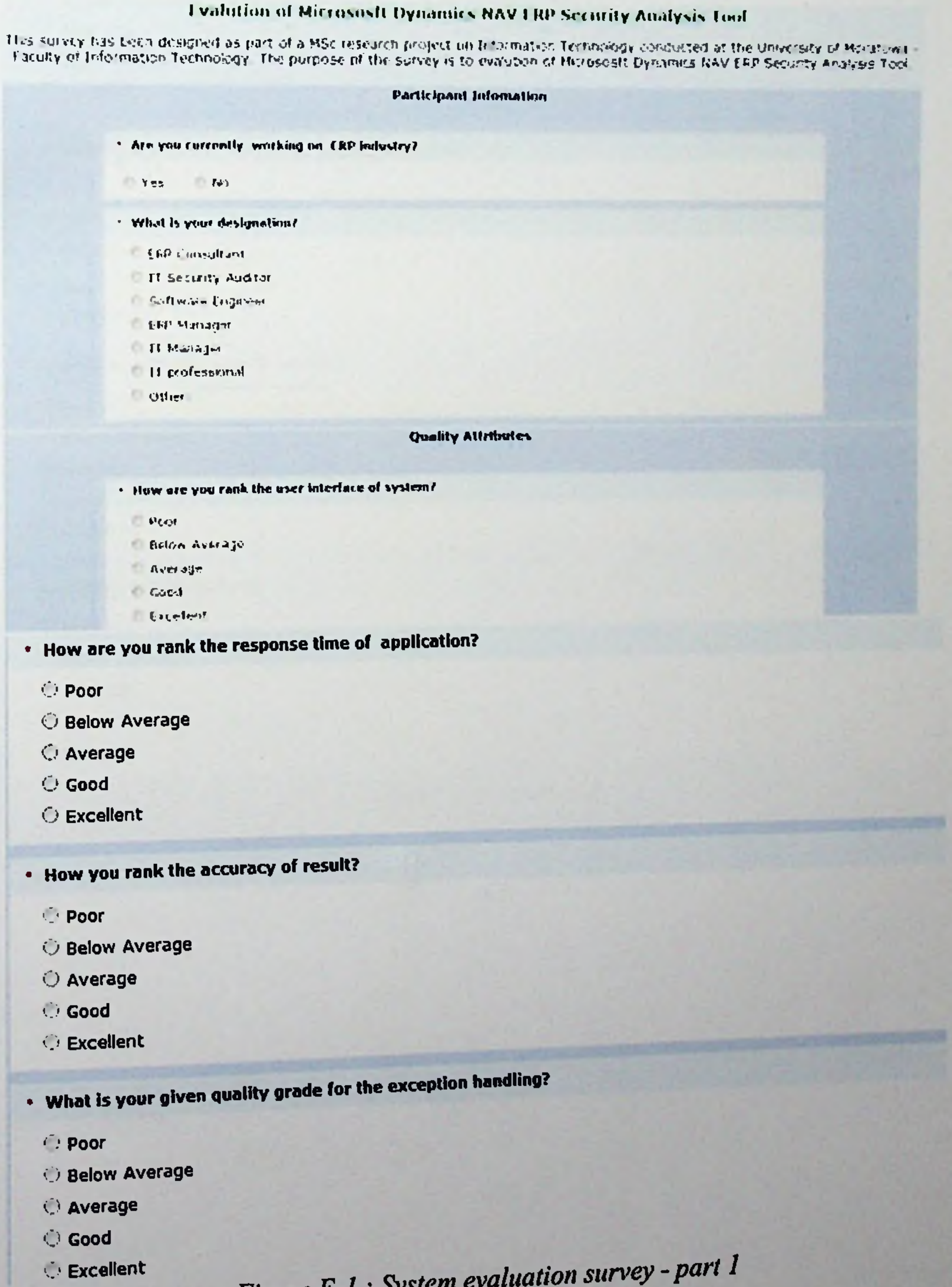
○ High Critical

○ Extreme Critical

Figure D-5 : Requirements analysis survey - part 5

Appendix E – Questionnaire used for evaluating the system

We have conducted an online survey using LimeSurvey to evaluation of our security analysis tool to check whether it was fulfilling the requirements.



Evalution of Micrososft Dynamics NAV ERP Security Analysis Tool

This survey has been designed as part of a MSc research project on Information Technology conducted at the University of Moratuwa - Faculty of Information Technology. The purpose of the survey is to evalution of Micrososft Dynamics NAV ERP Security Analysis Tool

Participant Infomation

- Are you currently working on ERP Industry?

○ Yes ○ No

- What is your designation?

○ ERP Consultant
○ IT Security Auditor
○ Software Engineer
○ ERP Manager
○ IT Manager
○ IT professional
○ Other

Quality Attributes

- How are you rank the user interface of system?

○ Poor
○ Below Average
○ Average
○ Good
○ Excelent

- How are you rank the response time of application?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

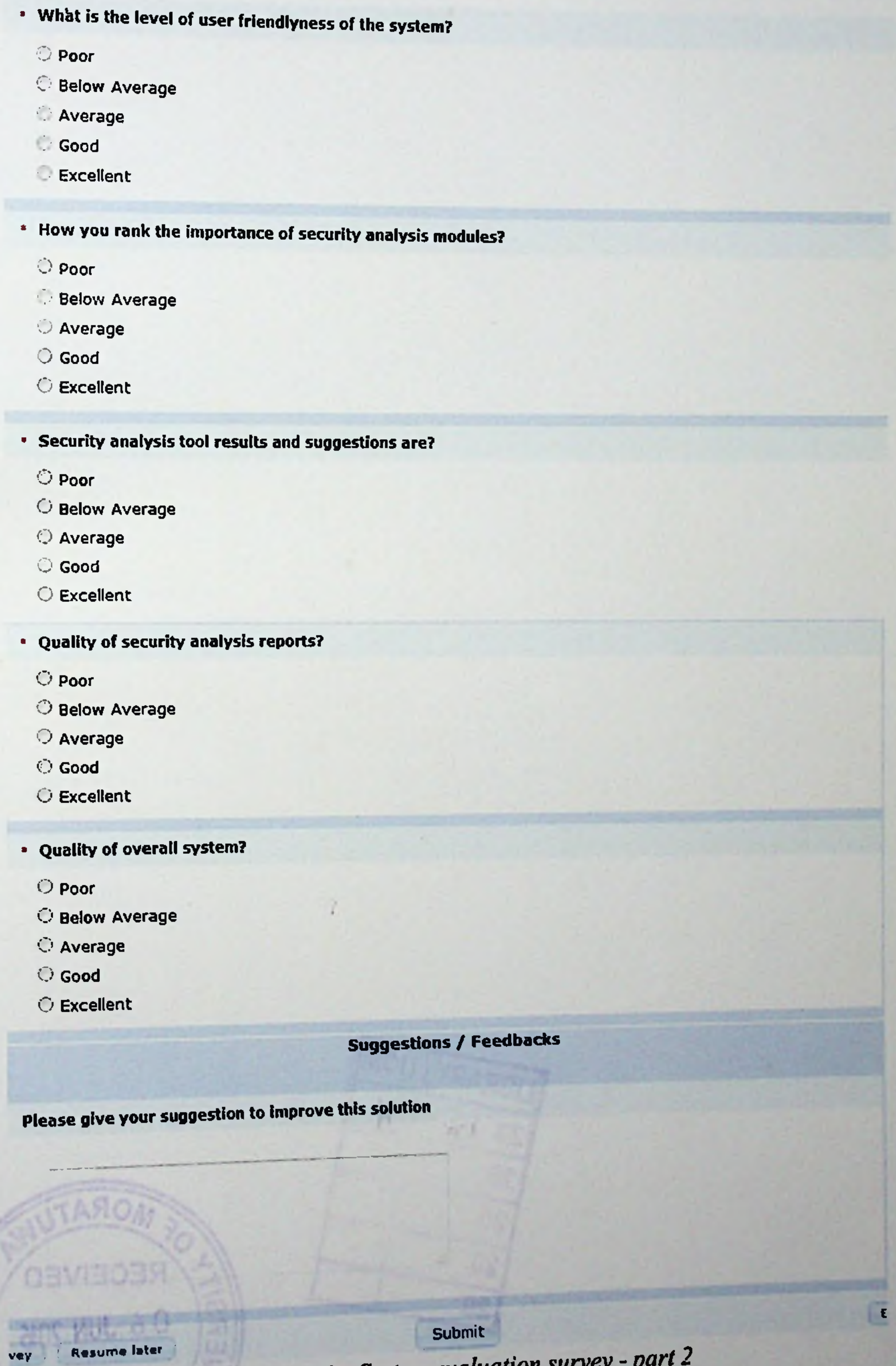
- How you rank the accuracy of result?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

- What is your given quality grade for the exception handling?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

Figure E-1 : System evaluation survey - part 1



- What is the level of user friendlyness of the system?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

- How you rank the importance of security analysis modules?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

- Security analysis tool results and suggestions are?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

- Quality of security analysis reports?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

- Quality of overall system?

○ Poor
○ Below Average
○ Average
○ Good
○ Excellent

Suggestions / Feedbacks

Please give your suggestion to improve this solution

Figure E-2 : System evaluation survey - part 2