INHAIMPLEMENTATION OF AUTOMATED SECURITY FOCUSED CONFIGURATION MANAGEMENT IN AN ACADEMIC ORGANIZATION THROUGH SCAP (NIST)

by

Sumayya Shahzad

A thesis submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindiin partial fulfillment of the requirements for the degree of MS in Information Security

June 2015

ABSTRACT

IMPLEMENTATION OF AUTOMATED SECURITY FOCUSED CONFIGURATION MANAGEMENT IN AN ACADEMIC ORGANIZATION THROUGH SCAP (NIST)

By

Sumayya Shahzad

Information system at large are at a greater risk than before by the hands of malicious attacker. The most overlooked is the configurations, with the efficient configuration managed and enforced by the organizations the lapses of security can be easily managed.Maintenance and configuration of multiple systems is an administrative nightmare and has resulted in multiple breaches of security. In order to defend any educational setting from external threats and to develop a coherent security fixated configuration management strategiesacompetitive and cost effective method is proposed. The technique in argument tightens the security of information systems in general. It'll profit an ordinary user and guises the intricacy of policy from them. It would cut the training costs of both the users and the implementers. The proposed system enables the addition and deletion of devices/hardware in an organization as it'll implement the same

policies pre-defined to a particular subdivision of systems. There are a limitation to the techniques proposed by SCAP in general and this problem is addressed in this thesis contribution.

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

_____

Sumayya Shahzad

DEDICATION

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my husband and teachers, who supported me each step of the way.

ACKNOWLEDGMENTS

All praises to Allah for the strengths and His blessing in completing this thesis.

I would like toconvey my gratitude to my supervisor, Dr. Baber Aslam, for his supervision and constantsupport. His invaluable help of constructive comments and suggestions throughout theexperimental and thesis works are major contributions for the success of this research. Also, Iwould thank my committee members; Dr.Imran Rashid, Assistant Prof Mian Muhammad WaseemIqbal and Lecturer Waleed bin Shahid for their support and knowledge regarding this topic.

I would also thank system administration team of MIS Cell of Military College of Signals, forproviding me with the required MCS nework related data.

Last, but not the least, I am highly thankful to my parents (Mr. and Mrs. M. A. Shahzad), siblings (Khizar, Sarmad) and husband (Ahsan Majid). They have always stood bymy dreams and aspirations and have been a great source of inspiration for me. I would like tothank them for all their care, love and support through my times of stress and excitement.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

1. Introduction

1.1 Overview

Whenever the term information system is used, there is a complex combination of hardware, software, infrastructure and trained personnel that comes into mind, which should be working together in an organized manner to make an organization complete its business goals. Whenever an information system is deployed it is assumed that it is not constant.Over the period of time, a particular server or a workstation requires multitude of configuration updates owing to the changes in the security policies or the advent of new threats/vulnerabilities. Configurations management is combination of business process/technological problem and it is definitely bigger than just tracking what changes an administrator can make for example, in a typical university of science and technology, there are a number of laboratories for technical aid of the students. These laboratories are equipped with the computer systems which may or may not be configured by domain controller. Laboratories are generally managed by individual administrator and typically there is no central control for the configuration management. Each laboratory has unique set of applications running hence requiring unique configuration management settings and rendering overall process of configurations management cumbersome and manual. Any hardware or software changes with respect to the business needs of an organization are a continuous operation. Whenever a change in information system is executed. It is most cases resulting in some sort of configuration management.

It is very easy for a malware to change the registry values. For example, a famous 2008 worm Conficker. When executed, the worm copies itself using a random name to the system directories folder. It modifies the registry key to create a randomly named service on the affected system. Hence making a deliberate change to the already available configurations [2]

The above example clearly illustrates how easily a malware can change the configuration of any information system (Desktop in this particular case). The information system security is most often compromised by the lack of configurations rather than the absence of security mechanisms. Hence, configuration validation is the topmost important operation in any organization to ensure the security. To maintain the configuration validations, there are a number of security policies, best-practices, and documentation of vulnerabilities. These are usually written in the natural language; hence to implement such policies and best practices is a manual and error prone process. Initiatives like the Security Content Automation Protocol (SCAP) ensure automation of configuration validation and the exchange of configuration information by providing a standard language [3].

the standard developed by NIST is dubbed as the Security Content Automation Protocol (SCAP) is a collection of standards the manages the smooth and standardized transfer of information related to the matters of software law. It is a framework which can serve multiple proposes that allow automated processes of configuration, vulnerability and patch checking. The development of SCAP include making security content related to management standardized, ensuring the system security products are interoperable and utilizing standardized content [5]. Many software vendors have developed tools based on SCAP's security standard notably are the IBM Tivoli Endpoint Manager for

Security and Compliance [6] and CA IT Client Manager [7]. These tools usually have one or two sub sections of standards for SCAP Implemented. These tools are not free and specifically designed for the specialized industry uses such as the US government and are not suitable for an academic environment. Since SCAP is not yet implemented for an academic institution that leads a potential need to be addressed. The current scenario will be very diverse in nature apart from the defense or government organizations. The current environment consists of multi spectrum security needs each needing a specific set of policy checks. For example, the labs entity of an institution requires lesser degree of security implemented in its systems than a faculty's official computer. The security needs are required to be clearly defined addressed and implemented using the NIST SCAP.

1.2 Motivation and Problem Statement

The technological advancement of recent year have yielded in multiple level of communication and information systems. Maintenance and configuration of multiple systems is an administrative nightmare and has resulted in multiple breaches of security. In order to protect any educational environment from external threats and to develop a coherent security focused configuration management policies an efficient and cost effective method is proposed. The method in discussion will tighten the security of information systems in general. It'll benefit an ordinary user and masks the complexity of policy from them. It would reduce the training costs of both the users and the implementers. The proposed system facilitates the addition and deletion of devices/hardware in an organization as it'll implement the same policies pre-defined to a particular subset of systems. There are a limitation to the techniques proposed by SCAP in general and this problem is addressed in this thesis contribution. The problem statement is "Developing a coherent solution to expand the

functionality of NIST's Scalable Content Automation Protocols with respect to the needs of an academic institution".

1.3 Objectives

The main objectives of thesis are:-

1. Study and understanding of SCAP.

2. To identify the workstations/servers information in the academic organizationand classify it according to the security severity needs.

3. To develop and write specific security configuration management policies with respect to standards provided by SCAP (Secure Content Automation Protocol).

4. To implement a tool like functionality to accept the SCAP defined policies and collect workstations information about a system being properly configured or not.

1.4 Thesis Contributions

This section provides the direct contributions from this thesis.

1.4.1 Survey of the current configurations process in leaning based information system environment

Conducting survey of all the computing facilities at an academic organization for effective configurations policy planning. This section would provide an in depth survey and analysis of the requirements for the automated configurations policy.

1.4.2 Categorization of security needs and configuration policy using NIST SCAP

After collecting and analyzing the survey data, the thesis would develop and write the security policies for the automated configurations management in a learning based environment. This section would be divided in to three parts i.e. user, power user and the administrator. The user in this case would be the students using all the computing facilities, the power user would be the teachers and the administrators would be those professional who need all the access to conduct the smooth managements of every day operations. The systems categorized aforementioned would be hardened by level of access and authority.

1.4.3 Development of proof of concept

The proof of concept automating all the policy enforcement would be developed and tested using the above defined policies as driving factor. The solution would not be developed as such to be limited to using only defined policy rather it would be allow room for further policies to be assimilated in itself.

1.4.4 Testing

The testing of the solution would be limited to checking how the system responds when a policy is changed and protecting against the unauthorized changes.

1.5 Thesis Organization

Organization of the thesis is explained in this section. The first chapter would be Introduction to the research problem and its solution. It would provide a basic standing for the solution. The second chapter of thesis would be the literature review, in this section current problems and their solutions

would be provided. Thirdly, we have the research methodologies in which various solutions have been methods of solving the research problem are addressed. In this there is a justification provided for the research methodology applied for the solution. At number four we have proposed policies for the SCAP checklists. At number 5 the solution is tested using various techniques and proof of concept is discussed. Lastly we have the chapter of conclusion and future direction of the thesis. After all the thesis chapters the appendix is also attached for further detail on the policies proposed.

1.6 Conclusion

In this chapter, the management of configurations and its limitation is discussed. Then the proposed solution and its objectives were thoroughly discussed. Lastly, the organization of thesis was discussed.

2 Literature Review

2.1 Introduction

Computers were born to facilitate the human brain to perform the calculation which the mind requires days to compute with errors executed in mere seconds. As the technology for the computers evolved so did the task assigned to computer systems. At first they played the role of giant calculators and as time went by the responsibilities and dimensions in which computers could be used increased. The added features means added programing and increased computing power. The programing or the mechanics behind the computers increased in complexity and layers. This increased complexity was the brain child of several computer scientist which may have resulted in some loopholes or backdoors. This gave way to the identification of those loopholes by malicious users and exploiting them for personal gains and what not. After developing and establishing the computer systems or collectively with the users or people identified with it is called the information systems, making sure they are secured at all times them came second. Now, with the increased complexity and layers which are part of the typical anatomy of an organization, automating the processes of security should be the optimum way of applying it and making sure that the configuration are up to date to compete with the increasing level of threats on the information system in general.

In 1973 report developed by the Defense Advanced Research Projects Agency (DARPA) established the connection of growing computer related crimes and the lack of the reporting on the matter. The earliest problems detected was the problem of maintaining a secure state of an operating system to software changes. However, it should be noticed that the integrity of the systems is dependent on the consumer only and there is no mention of vulnerabilities or malicious program [11]. It was not until 1986, the world encountered a virus called brain which was created by two Pakistanis to deter pirated copies of the software created by them. The virus spread on floppy disks and infected the boot segments of IBM personal computers. It was sophisticated enough to remain hidden in the memory of PC [12].

The main problem still remains how to protect a computer in an increasing complex scenarios today. For this purposes, one can take many steps which can also be instinctive and intuitive. Publicizing the idea of secure surf, installation of security patches and effective configuration of computer and firewall are one of the few steps to assure security in prevalence of malware-ridden world. This may be easier for a single user or workstation but it becomes difficult in larger organization with multiple levels of workstations and servers work together. The main challenge in aforementioned scenario still remains how to effectively protect the large information from the outside threats. Before moving on to the next step, it is important that the definition of malware is identified:

> *"**Malicious software** is any **software** that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, Trojan, adware, spyware, root kit, etc.* [13]"

The technology was not as connected in 1970s or 80s as it was from the 90s and the constant revolution of interconnectivity has led to the standardization of computer systems. At first, there were a number of systems like mainframe, minicomputer and personal computer which used different processors like Motorola, HP, IBM, Sun and AMD to name a few. Different processors meant different architectures which in turn reduced the effects of malware to a smaller population compared to the broad-spectrum effects today.

The malwares can be broadly classified in to three distinctive categories Trojan, Virus and Worm. More and more terms are coined every other day to mimic the behavior of specific malware like ad-ware, ransom-ware and spyware etc. but these are not the scope of our document as it only addresses to the behavior exhibited by the malware regardless of its type. Adware, Trojans and Spyware most of time are executed and spread using the web browser only. Web browsers can be made secure with the help of sandboxing technique. Worms can also be of varying types such asIRC-Worm, P2P-Worm,Net-Worm, IM-Worm and Email-Worm to name a few. Interested reader can look into [18], [19] and [21]. Most of the worms propagate through various exploits in the networking programs or networks. The mechanism of its circulation is out of the scale for this document. The methodical feature of the payload accessing the configurations and registry is of interest. With the progression of the sophistication level in the Intrusion Detection System (IDS), the network traffic can denote the pattern of proliferating of worms and viruses through semantic, heuristics or pattern matching. Fundamentally the mission of viruses and worms are the same, which is to rule the world of computers by making all the computers infected. But, the eco system of a virus is different than a worm, a virus needs to attach itself either to a part of an executable or to

write itself in the boot which may result in the corruption of the system files hence, the user is unable to reach the computer. Both virus, worms and Trojan horses contain the payload, which waits to be triggered at a specific time, or a command by the developer to carry out the mission assigned to it. Interested readers can read more about the viruses in [20], [22] and [23]. While there is a lot of research on the quantifying aspects of malware like the size of the botnet [15], executables figure infected with malicious code such as a spyware[31] [32] and the number of mischievous websites that have adware etc. Another study is about the various techniques like honeypots from which to lure and trap malware for study. But little is known what a malware does to a native operating system, information about the hosting systems of program files and network. For the collection of malware analysis, the tool Anubis is proposed as it is freely available as a service and it doesn't require computational requirements.

There is an online software which is not exposed to the end user called "Anubis" and its run and developed by Lastline Inc and System secure lab [16]. It collects and analyzes virus binaries/executables submitted from all over the world by computer professionals, honey bot and various resources. This tools specializes in analyzing what changes are made to a typical windows host computer operating systems when infected by a malware. That includes the registry processes or the calling of Windows API calls, vital system and path of the data movements and archives of the network data in a typical computer system. In return, the afore-mentioned processes provide a completeinterpretation of harmfulmovementswhich may not belikely wheneverobserving network traffic unaided which is the case of Intrusion Detection Systems (IDS). The goal of this thesis is to provide effective protection against the configuration changed by either a malicious user or a

malware to remain unaffected as well as automate the processes submitted by SCAP NIST which will help streamline the processes typically part of an organization's business processes. While the analysis provided by [14] the following is the listed observed behavior by a malware.

2.2 Typical Behavior of a Malware:

To infer the typical behavior of the malware. It is important to consider the data set used by the malware for analysis. Since a large number of data set would be the greater indicator of inherent patterns, which could be the assurance of typical behavior. Anubis collects malware through the public web interface and a sum of supplies from the honey pots, web crawlers, spam traps and by security companies or analyst of the affected machines. The data set used in Anubis in [14] contains total of 901,294 unique samples based on the MD5 hashing algorithm from a total of 1,167,542 submissions. A sample is analyzed only once by the tool due to restraint resources. The tool is only used to document the Windows native system calls and Windows API functions that the malignant program incites. Since the submission of malware to this tool is free, hence there can be a number of irrelevant files for people who want to test the online system. The submissions of the PE (Portable Executable) files amongst the data set is categorized as follows.

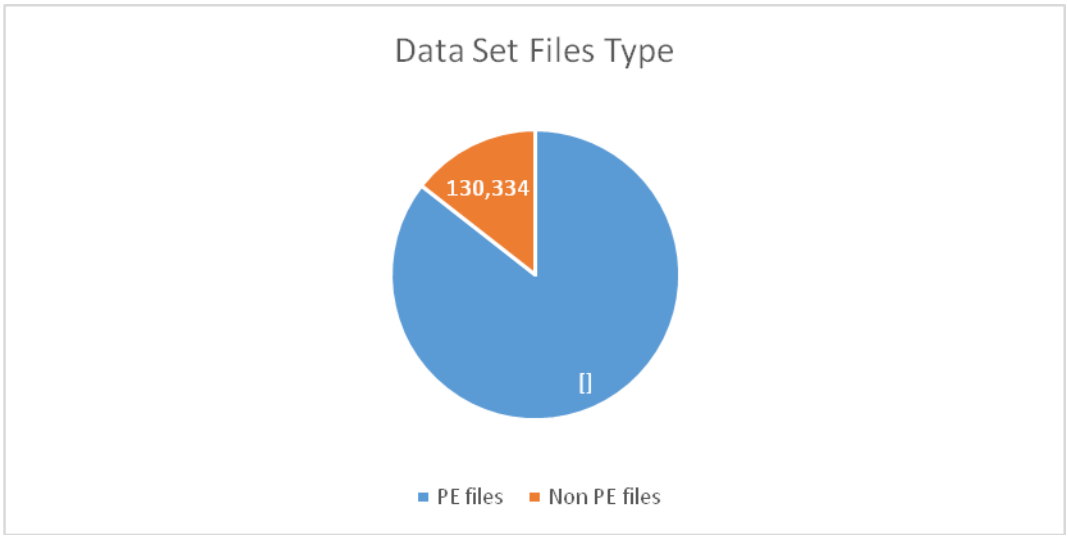

Figure 1 File type dataset

The classification of PE files amongst the data set is as follows

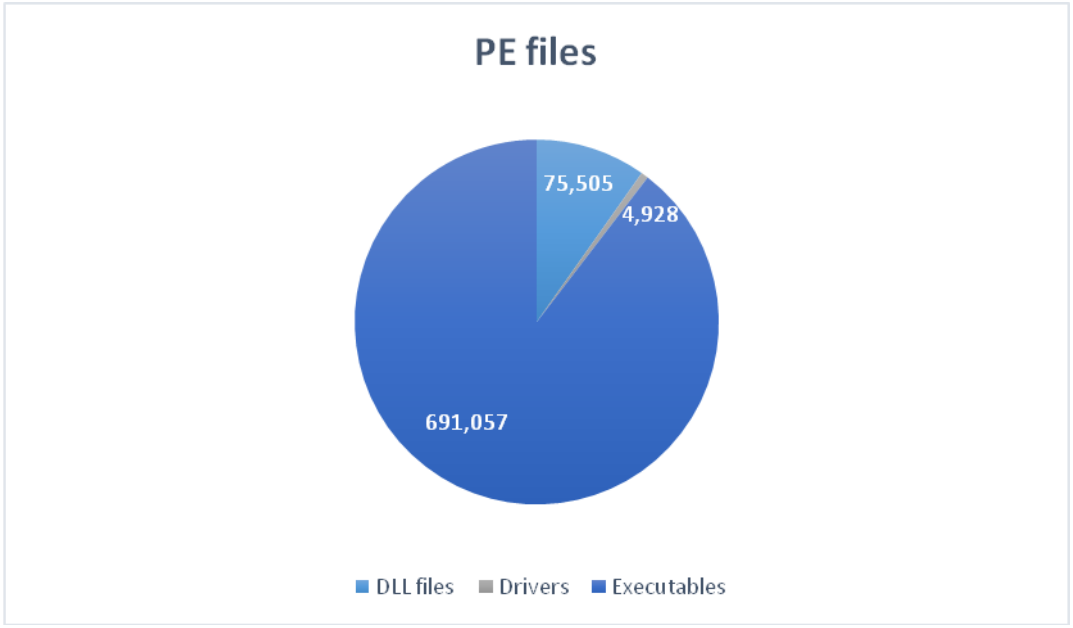

Figure 2 PE Files

The classification of Non PE files between the data set is

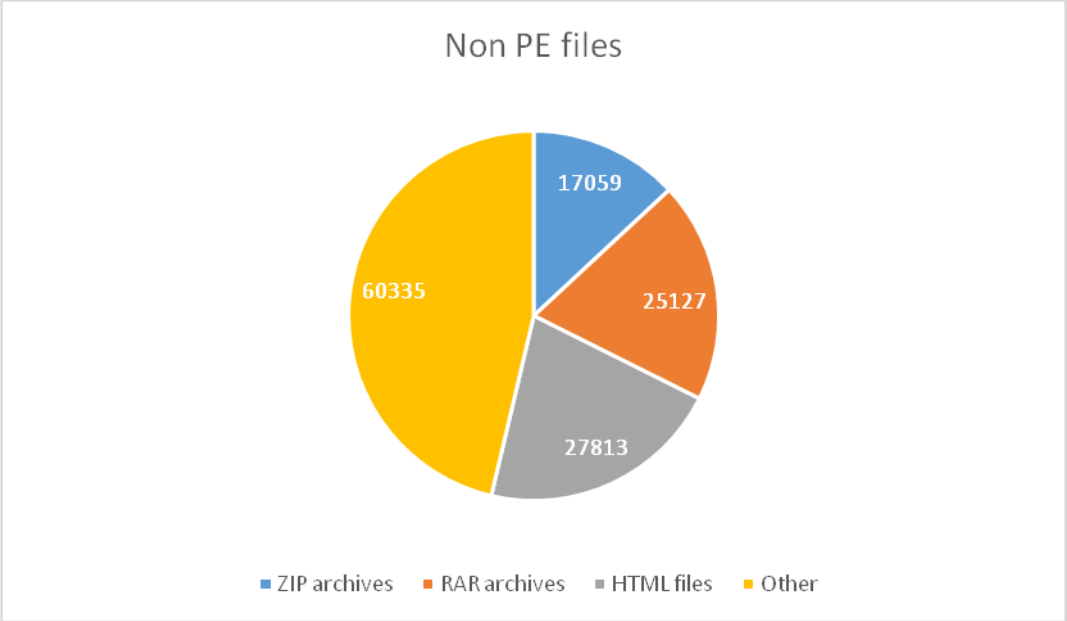

Figure 3 Non PE files

2.2.1 Observation Based on the PE Files

After collecting and analyzing the dataset of a malware which narrows down to 770,960 files among the total of 901,294 unique sample. The finding can be divided into three distinct categories, i.e. typical behavior overview, Auto-start Locations and Registry activity. There is also a file access activity which is not included in the scope of this document.

2.2.2 Typical Malware Behavior Overview

Sorting of the observed behavior is

Installation of a windows kernel driver: Kernel mode framework is developed on the notion of sharing a single virtual address space. Which means the installed driver can interact with

other drivers and Operating System (OS). The installed driver, if malevolent can overwrite the files of the OS, hence rendering the system useless and compromised.

1. Installation of a windows service: Microsoft Windows services, enable a user to install/create long-running executable applications that run in their own specific Windows sessions. These services can be automatically start when the system boots, can be paused and restarted, and do not show any form of Graphical User Interface (GUI). These are powerful system privileges, when unmanaged can yield in to big disasters e.g. transformation of a system into a bot for a Distributed Denial of Service Attacks.
2. Modifying the hosts file: the file normal present in the C:\windows\system32\drivers\etc\hosts and adding records in it can map the Internet Protocol Addresses (IP) to host names. If an attacker wants to run some automated script or process that uses a live domain name e.g. any commercial company registered on a domain, it can modify the host files such that can be misleading and may lead to the phishing and pharming attacks.
3. Creating, modifying or deleting a file: A Trojan looking for updates can be creating temporary files in C:\Users\User Profile\AppData\Local\Temp. A virus may delete critical files to maximize the damage to the Operating System. Lastly, a virus may need to modify executable files to make a system infected and repeat the process for replication.
4. Display a GUI Window: Some viruses have hidden root cause of activism such as human rights, or women rights and may be terrorism. For these, the payload of a malware should be displaying a GUI window to display its message.

5. Network Traffic: A malware propagating in a network would be leaving an evidence trail of data in the form of network traffic. Which may help an Intrusion Detection System (IDS) for catching the malicious code.
6. Writing to stderr and stdout: this is same as the aforementioned point 5. Instead of the screen, the information would be output as command lines in command prompt using standard streams, stderr (for error message) and stdout (write information)
7. Modifying, creating a registry key: registry is the hierarchical database of any operation system that contains all the information pertaining to the configurations of the windows operating system. A malicious code in under any circumstances should not be changing/creating the configuration setting of the operating system.
8. Creating a process: A process is an occurrence of a program in execution. A process is like a small chunk of a program designed carryout a specific task. A program can consist of many processes. In this case, the developer behind the malicious code would divide the program into smaller processes to evade detection. The inventor can also leech to an existing process to carry out specific tasks such as use of explorer.exe to use 100% CPU processing time.

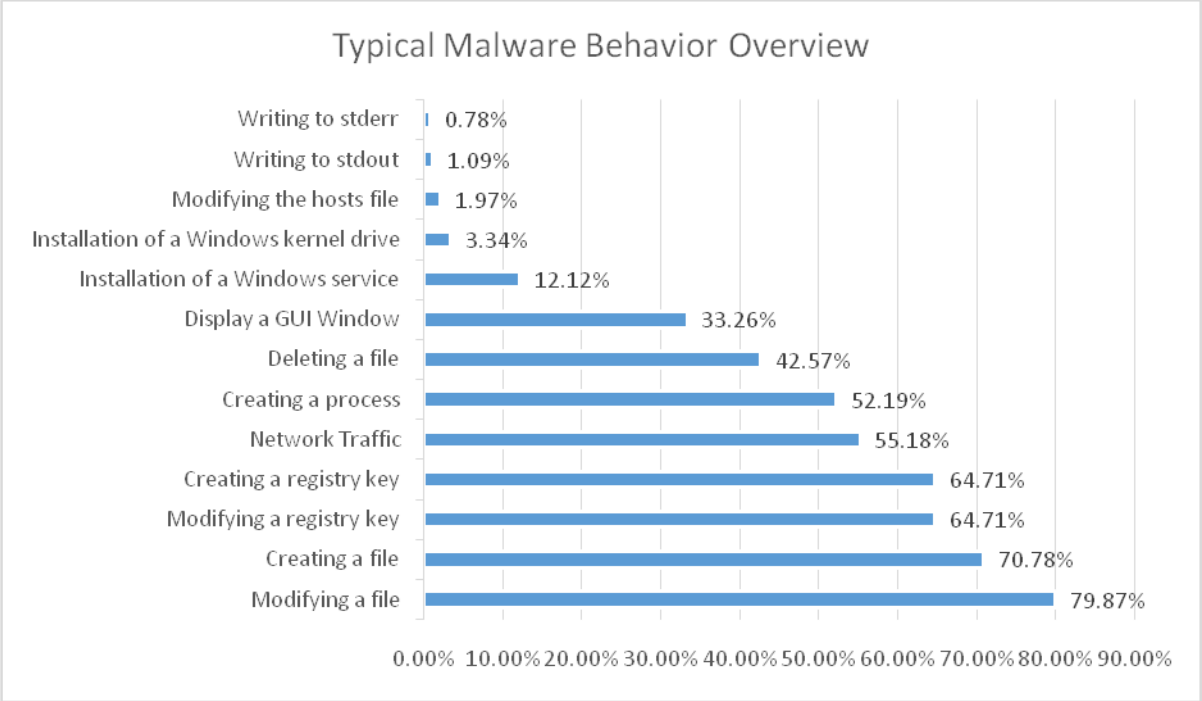

Figure 4 Typical malware behavior overview

The explanation of the figure above is stated prior to the display. However, this figure indicates the most common behaviors of a malware once it infects a system. The most common type of malware behavior is that it always tries to modify the file be it any executable or a host files. The modification and creation of file are a generic behavior. An operating system cannot survive without constantly reading, writing and modifying a file. However, modification of registry key and creation could be monitor for potential malware lurking in the depths of an operating system.

The scope of this documents concerns with the automation and configuration management of the registry keys in a windows operating system. So, the next analysis is of utmost importance, the program with malevolent intent always tries to make sure that it is able to run whenever a computer starts. There is a specific type of virus that tries to write itself to the boot sector of the OS, thus confirming the ticket to automatic loading while booting up. There is another method through which

a malware assures its persistence, the auto-start locations of registry. The tools has gather the top locations of auto-start portion of the registry and has calculated the percentage out of the total samples of the malware files dataset. E.g. only 17.53% malware created a registry key in the following location HKLM\System\Currentcontrolset\Services\%Imagepath out of the complete data set. The critical ambition of any program with malicious intent is to make sure it keeps running when the computer starts or reboot. Auto Start locations in any operating system are the key attractions for any malware. The auto start in windows 7 are following

- For a current user the auto-start location inside windows would be

  C:\Users\"User"\AppData\Local

  Where user would be username e.g "Tom", "Ali" etc
- For all the users in the computer, settings could be located in

9. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

The auto-start locations in the registry would be

- For Local Machine

  1. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr entVersion\Run

  2. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr entVersion\RunOnce
- For Current User

  1. HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\Run

  2. HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\RunOnce
- Other Paths

1. HKU\ProgID\Software\Microsoft\Windows\CurrentVersi on\Run

   systemdrive\Documents \All Users\Start Menu\Programs\Startup

2. systemdrive\Documents \username\Start Menu\Programs\Startup

3. The top 10 auto-start locations chosen by the malware as

   follows.

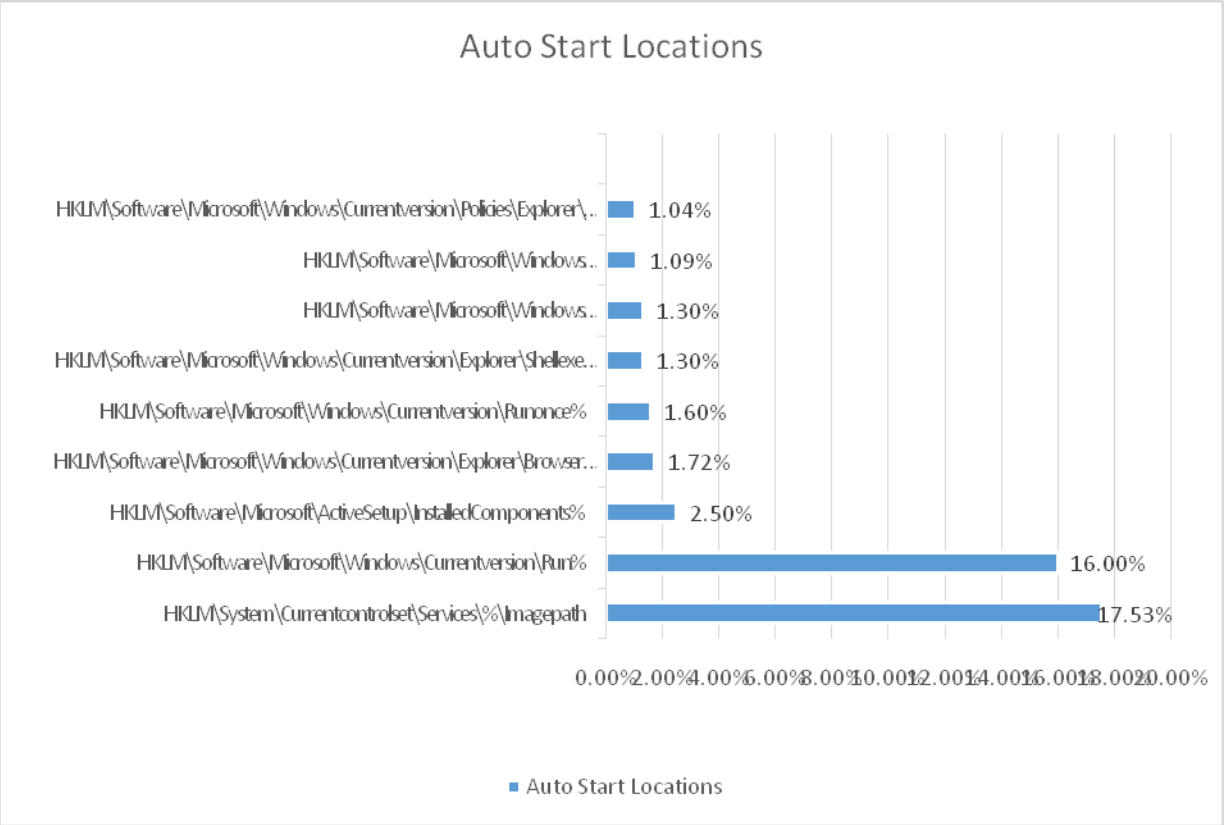

Figure 5 Autostart Location

The registry behavior observed is depicted below in further detail. The practice of displaying the analytical data is the same i.e. to calculate the percentages of the malware portraying the specific key behavior.

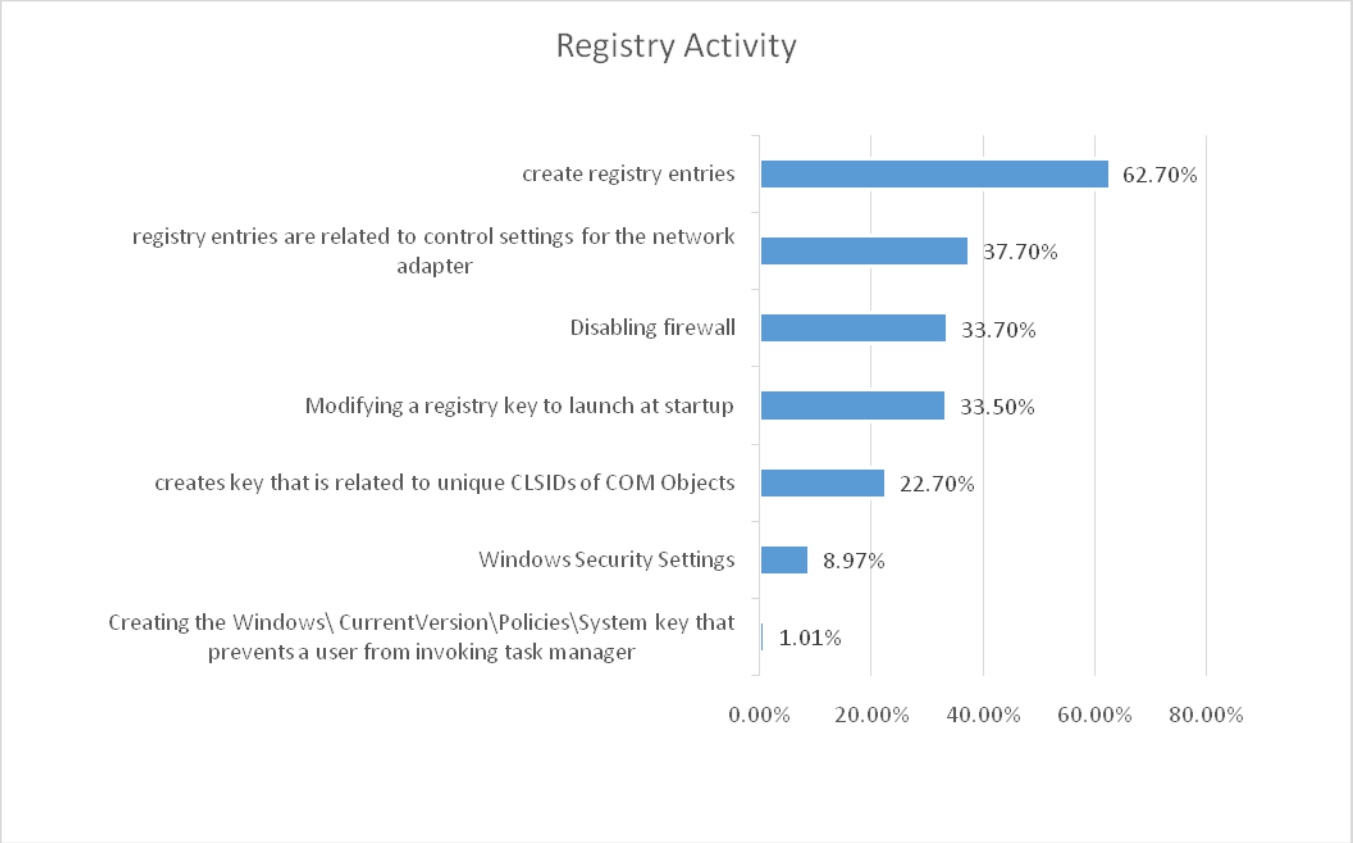

Figure 6 Registry Activity

It can be concluded from the above figure, the most common behavior of a malware is to create registry entries, making entries pertaining to the network adapter for a good communication with command and control center and to disable a firewall.

By maintaining continuous updates and software patches, it is possible to key malware at bay but the problem cannot be fully eradicated if and unless, a way is found out to constantly maintain the optimum configurations required for the upkeep and maintenance of computers in a large network.

2.3 Importance of Windows Registry Integrity

In [33] it is stated that the windows registry can be the single most vulnerable component of an operating system. Since, the registry stocksmassivequantities of complicated, undocumented and defenselessorganization of data. If a malware destroys a registry, the task of its undoing is cumbersome and crucial to system and applications developer. Windows registry encompasses a classifiedcommunaldepot for the called and entered configuration data. This data is equallydistributed and opened by the operating system and applications. The storage of the registry can easily distinguish between per-user and system-wide settings. The keys in each registry for a particular system can be view as files directory that can contain sub-keys (sub-folders) and a registry item (file) that contains a key piece of computer configuration.

Researches at Microsoft analyzed the frailty of the registry by extracting data from the Product Support Services (PSS) and the problems posted on the web forums. The problems in the data set were recreated using STRIDER Troubleshooter for analysis purposes [34]. For the PSS data set problem in which a sum of a large number of problem were documented, numerically 2,400,000 problems of which approx. 143,157 Registry keys/items. Hence, a rough estimate of around 4.4%

2.3.1 Registry Problem Indicator

There are seven key problems identified by the Ganapathi, Wang, Lao and Wen after the loss of integrity which can be categorized in the form of table as follows

Table 1 Problem indicators in registry

Problem	Description
Unstable/unusable system	Specific Registry bad configurations are the reason ofharshdamage of acuteperformance and/or exposedpathsaimed at the operating system towards giving in.
Cannot perform a function or action	There are times whenever a systems user is unable to perform specific task such as email or web surfing.
Unanticipated side-effect	Specificaffects by registry tampering are instigated by unhealthyapplicationscheme. Additionally, what is considered normal may undermine the normal function of user resulting in loss at some functionality For example, some new program installed by the user messes up the enumeration of the volumes in any operating system. While this may be harmless, can pose dire effects.

Problem	Description
Cannot locate user interface to perform a task	There are times whenever an interface is hiding behind many layers of menus. In this case, we will take an example of IE asking whether it should save a particular user's password. If a user selects this then it is difficult for them to restore them back because it has so many levels.
User interface disappears but functionality is preserved	Sometimes the UI can be absent or maliciously tampered with. in this case, restoring through command line might not be effective especially if the related registry key to the UI is deleted.

Program adaptation or automation is performed in an unexpected manner	There can be scenarios in which the decision for automation may be counterproductive for the user. If a person want to resume slideshow of its presentation. The computer can display it incorrectly based on the incorrect registry keys reading a second output screen.

The above table can be represented in the form of a pie as well to exhibit the share of the most common problem found by compromising the integrity of a registry.

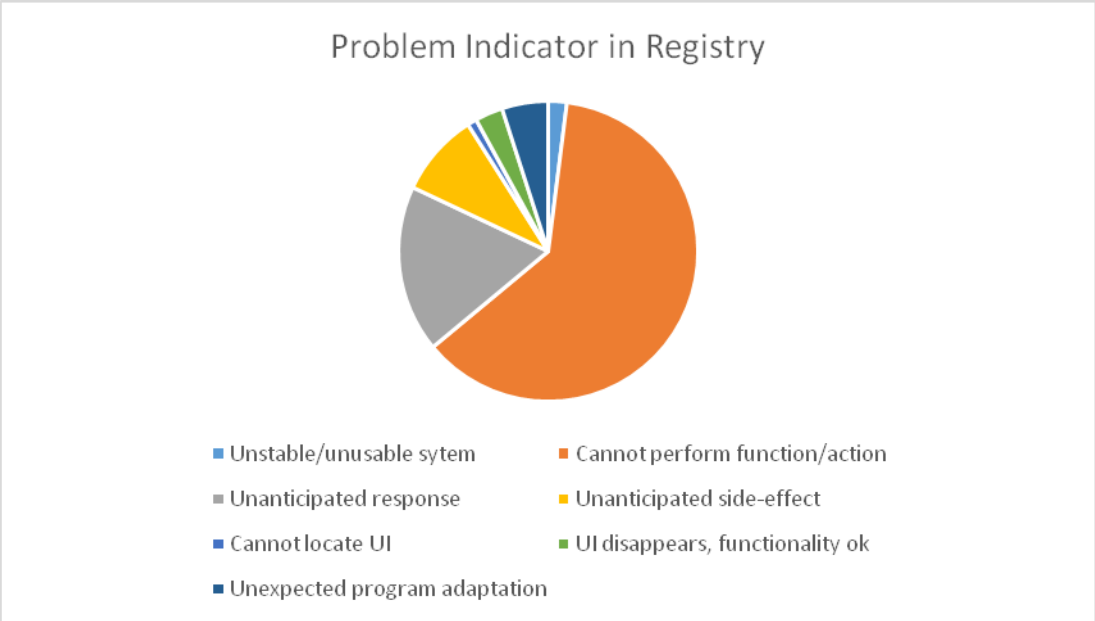

Figure 7 Problem indicator in registry

2.3.2 Impact of Registry problems on a machine's functionality

The level of impacts can be categorized into two distinct types

1. System-wide or affecting only a particular user, clearly the winner between the two is system-wide problems. However, it is further noted that most of the mistakes are made in updating and creating of a new registry key be it by developer or malwares.

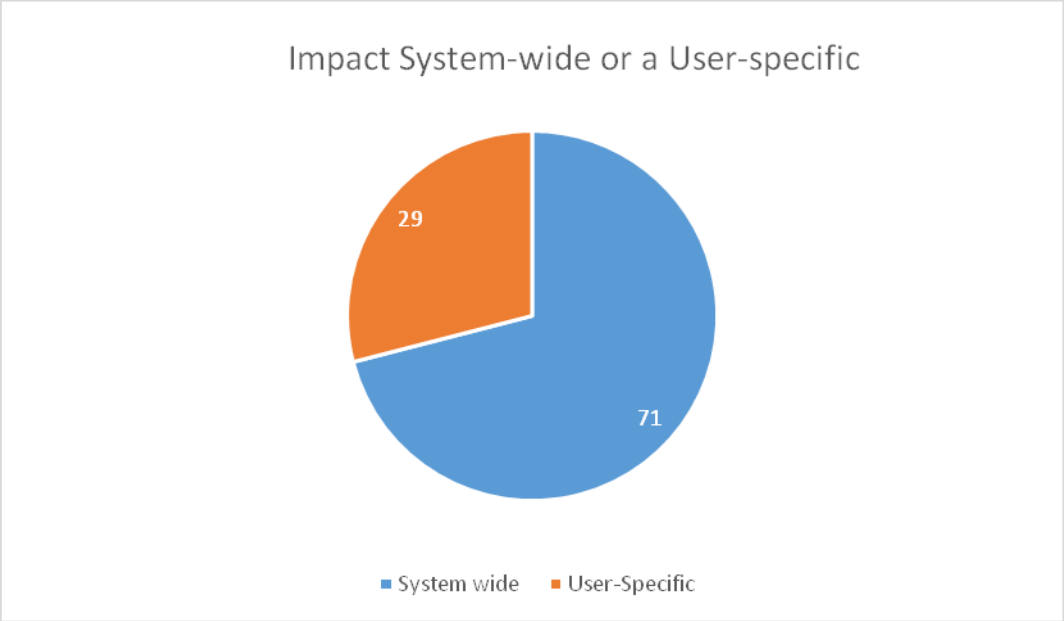

Figure 8 System wide Impact

2. Problem effecting a single application, multiple applications or system level- in this case it is exhibited, that out of the data set of almost 5,379 cases of PSS, almost 40% of the

corruptionis intended to make system level problem which is indicated in the chart below.

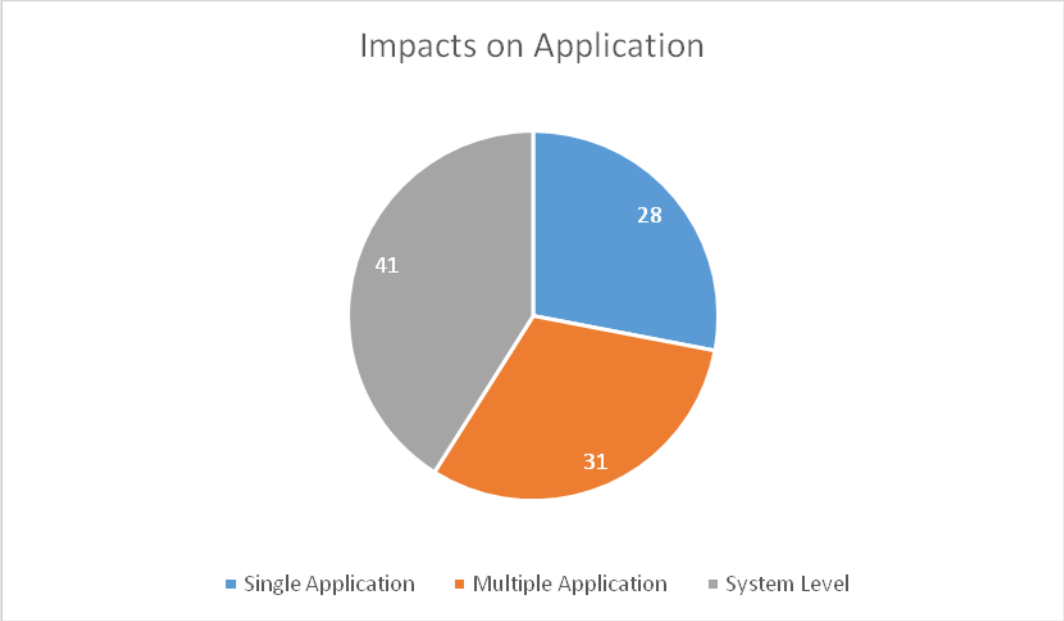

Figure 9 Impacts on application

2.3.3 Related work on the Windows Registry Integrity

2.3.3.1 Context-based Online Configuration-Error Detection

In [35] the authors have proposed a new technique to combat the accidental or intentional registry changes that may limit a computer's complete usability. The authors also maintained since the configuration data is highly dynamic e.g. on average 10^4 average writes to Registry per day per machine. Out of which 10^2 are to the frequently accessed Registries that have never changed before. A tool like functionality nicknamed as CODE is proposed, CODE basically collects all the changes to the registry and tries to build a context out them.

A motivating example would be, a real-world configuration error happens in which the automatic updates of windows are disabled like most of the users. The error was caused by the user when

removing a program he/she thought extraneous. Typically, whenever a program tries to access registry, it does so in specific number of sequences. Those number of sequences can then be divided into rules. Any of the rules violated can then be calculated and logged as an error. For example, svchost.exe is a process on computer that hosts, or contains, other individual services that Windows uses to perform various functions like the checking up on the windows update server for software update. Typically, that process is conducted exactly 45 accesses to the registry. If the windows updates are set to "NoAutoUpdate", then process executes with 27 accesses to the registry. Since, the typical behavior would be to have 45 accesses rather than 27. The CODE will detect an error. The context is built by categorizing the general rules. The CODE then uses these context-base rules to determine the problem and remove the error.

It is starkly different than the thesis idea proposed here, since the idea of this thesis is make sure the security configurations are not reset by any user or malware. The tool proposed above is trying to generate a 'context' behind every registry change hence, controlling configuration changes by establishing some rules.

2.3.3.2 Detecting Malicious Software by Monitoring Anomalous Registry Accesses

The system proposed here is based on the PHAD (Packet Header Anomaly Detection) that will act as a host based anomaly detector. Packet header Anomaly Detector works on generating a model of the network based on normal traffic. If any packet containing bogus IP or port number is detected. It is deleted or not forwarded to the host. The authors Apap, Honig in [35] has determined a way novel way to apply the customized PHAD to the anomalous registry accesses by the malware or malicious software. In this technique proposed the model is trained on the clean registry accesses data of the

host computer. When the model is specifically trained, any of the accesses deviating from the normal model is considered an anomaly, hence rejected from the host system. The proposed system is divided into three distinctive parts i.e BAM (Basic Auditing Module), Model Generator and the Anomaly Detector. BAM uses the registry reads and writes as an auditing module in which the WIN32 registry is hooked to a log file where all the registry transactions are saved. BAM then translates the files into a file database as a source for the Model Generator. A model generator then uses the data source to generate the normal network model and lastly, the model is used by Anomaly Detector as a normal flow of data.

Limitation of this detection model would be that it generates the initial model on the assumption of having clean or malware free data in realistic models it is quite hard to determine. Additionally, the program proposed does not have a lot of false positive like the context based technique proposed. This program also does not deal with the security policies of any computer system and does not strive to make a computer safer by maintaining or organizing its security policies.

2.4 NIST SCAP

The information security needs of an organization increases exponentially as the organization increases its services and operations. The increase in operations, increases an organization's susceptibility to competition. The organization requires to constantly protect its assets from theft, espionage and blackmail. One of the more prevalent problems is the lack of configurations which may lead to the different vulnerabilities. The accomplishment of these requirements is a time consuming and error prone process as the weakest link in security is general humans. Organizations lack standardized ways of performing the security processes and reporting. Standardizing of assets

for example, an intimidating process that needs to be constantly updated and should be properly referenced in all of the reports. In addition to the aforesaid, tasks like security assessments, decision making and vulnerability remediation are one of the many tasks that need to be standardized and automated.

To overcome the menacing task of security automation, National Institute of Standards and Technology has developed the Security Content Automation Protocol (SCAP) [17]. SCAP is planned to organized, express, and measure security related information in standardized ways, using model reference data, such as identifier for software flaws and security configuration issues. SCAP can help maintain the security of enterprise systems by automatically verifying the installation of patches, checking system configuration settings and examining systems for the signs of compromise.

NIST's website contains a lot of details on how to execute the SCAP on an organizational level. The most applicable in the scope of this document are The Technical Specification for the Security Content Automation Protocol (SCAP) Version 1.2 [24] and Guide for the Security-Focused Configurations Management of Information Systems [25].

SCAP contains various sub specifications such as

1. XCCDF is a specification language for scripting security checklists, benchmarks and associated type of documents. Specific type of XCCDF document signifies a organized group of security configurations rules for set of target information systems. Requirements is designed to support information exchange, document production, administrative and conditional shaping, automated compliance testing and compliance scoring. The specification also states a data model and format for storing results of a benchmark compliance testing.

XCCDF documents are written in XML, and maybe validated with an XML Schema-validating parser.

2.OVAL stands for open vulnerability and assessment language. It is a standard language to ensure effective communication, interoperability and standardization of vulnerability information across multiple platform. It is developed in XML (eXtensible Markup Language) for the standardized transfer of information. The repository of vulnerabilities is written in OVAL so that any XML parser can read and identify the language. OVAL can describe various machine states depending on its repository as vulnerable, non-compliant, installed asset and patch.

3.OCIL designs a structure for expressing a set of questions to be presented to a user and equivalent measures to understand reactions to these queries. OCIL is by no means confined to IT security. Other possible uses include research inquiries, academic course exams and instructional walkthroughs. In the information system security, organizations work with the security policies that point the information need to be made secure and the minimum security requirements that must be met in order to make sure the information is protected to the maximum.

4.CPE stands for Common Platform Enumeration Dictionary. It is a structured naming arrangement for information technology systems, software and packages. It is based on the broad composition for URI (Uniform Resource Identifiers). CPE includes a formal name format, a technique for checking the names against a system and a description format for binding text and tests to a name.

5.CCE is Common Configuration Enumeration which as the name suggests is inventory management specification for the proposed configurations of information systems. The CCE is important for developing a database against baseline configurations which can act as remediation for common vulnerabilities found. The specification is based on XML. Since in any organization, there can be multiple information sources which need to be standardized to make effective and long term security planning. CCE provides a liaison between humans and computers with text intensive description for the former and the machine readable code for the latter.

6.CVE is Common Vulnerability Enumeration is an XML based inventory system for the vulnerabilities found commonly in the target information system. The CVE is then utilized by other components of SCAP such as OVAL etc. It can bring coherence and standardization to the entire specification.

7.CVSS (Common Vulnerability Scoring System System) is a scoring system for interconnecting the features and impacts of IT vulnerabilities. It is a quantitative model that ensures the repeatable accurate dimension while enabling users to see the fundamental exposing qualities (vulnerabilities) that are used to produce results.

8.CCSS stands for the Common Configuration Scoring System is a scoring system developed for interconnecting the influences of misconfigurations in the IT systems. It like CVSS is a quantitative model that is ensuring the precise measurements of misconfigurations while enabling the stake holders to see the configurations that are used to yield this result.

The purpose of this thesis would be automating the controls of NIST's SCAP configuration controls. A control is said to be automated if the process can be done without the intervention of humans. The controls are said to be partially automated if they still require human intervention. Following is the discussion in the limited automation originally of SCAP Security Controls.

2.4.1 Limitation in Automation of SCAP Security Controls

In [26] there is a comparison of automation controls between numbers of Information Security Controls. The authors Montesino and Fenz have chosen three types of security controls i.e. ISO 27001, NIST SP 800-53 and Consensus Audit Guidelines. For the following analysis, a security control can be automated if operations are conducted without the intervention of human beings. It was noted that not all the security controls could be automated, some could be only partially automated. The data for the NIST SP 800-53 is as follows.

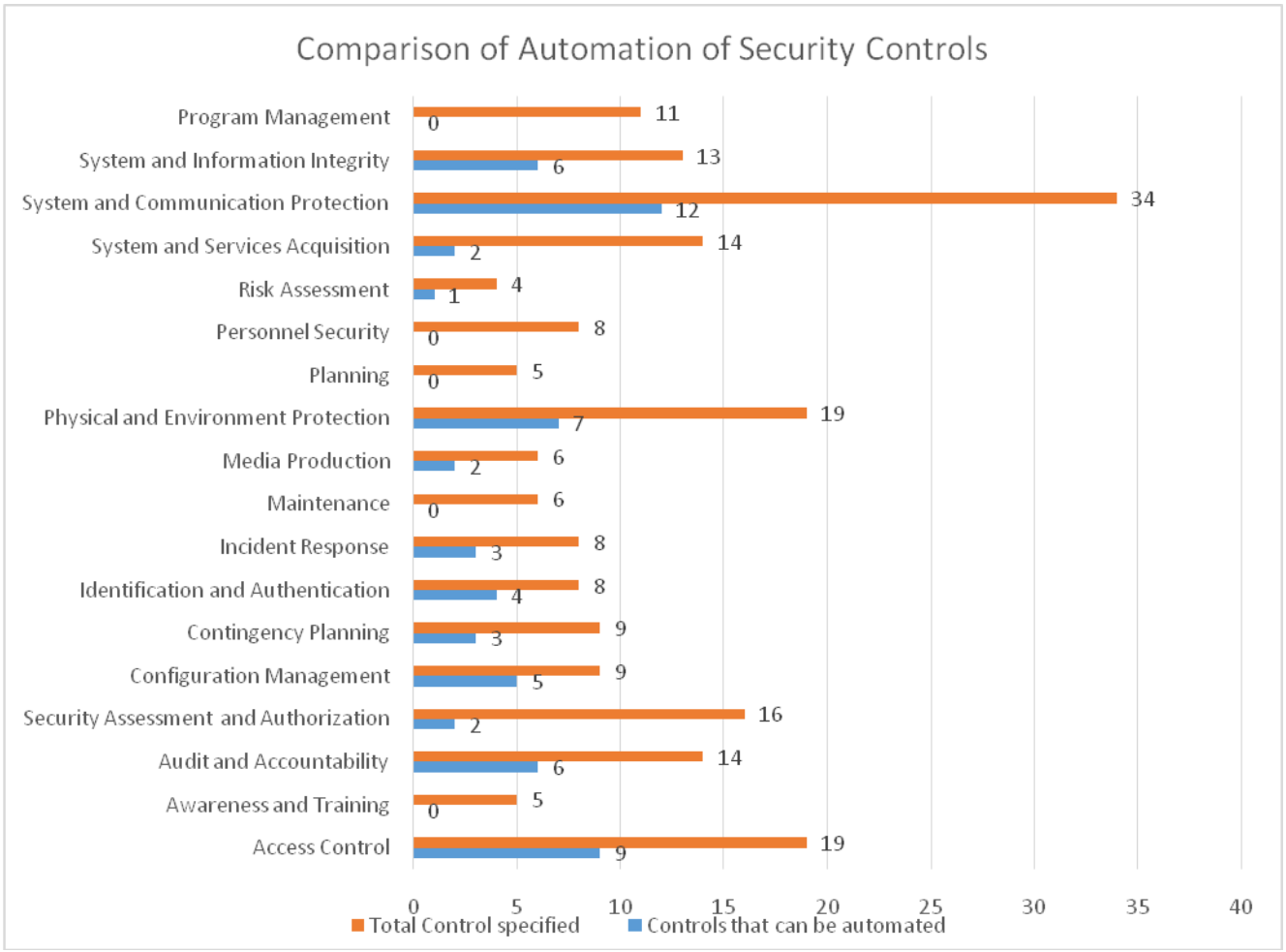

Figure 10 Automation of Controls in SCAP

Since the above figure denotes all the controls provided by the NIST SP 800-53, the controls can be automated are highlighted in blue and the ones can be automated are highlighted in orange. It is observed from the above figure that most of the controls cannot be fully automated without the intervention of humans. The above figure has all the security controls defined by the SCAP but our concern only deals with configurations management in an organization. Configuration management has total of 9 security controls out of which only 5 can be automated. The remaining 4 would be automated and the results would be shared at the end of this document.

2.4.2 Other Solution Utilizing NIST SCAP

2.4.2.1 SCAP Based Configuration Analytics for Comprehensive Compliance Checking

In [30] Alsaleh, Noraden and Al-Shaer proposed a new technique of combining the compliance checking module at desktop level with the network configurations resulting in a coherent solution much like a logical language for comprehensive networks and computers based analysis. In other words, the paper has suggested that the combining the configuration automation controls in the desktop level when combined with network level configurations can result in a more end to end security analysis. This technique does not alter or enhance the automating capability of SCAP NIST like this document would be proposing. Rather, it would take the original specification and user it to create a configuration checker dubbed as 'ConfigChecker' and combines it with the network configurations. The tool developed has a query layer that will allow a system administrator to perform detail analysis on the network it is working on. For example to check whether the following computers contains a specific security configuration, the system administrator would be able to view that. The solution differs remarkably than the technique proposed in this document. This document focuses only on enhancing the security control of the NIST SCAP configuration management. It would be aiming at automating the configuration management without the complete human intervention.

3 Research Methodologies and Analysis

3.1 Introduction

In this chapter, the problem's scope would be narrowed down. Initial survey of the problem's extent would be analyzed and the solution would be tailored according to it. From the beginning it has been established that the problem of configuration management would be addressed to the academic challenges. There are no exquisite budgets to protect the organization's assets from a disgruntled or bored employee or student. Hence, a cost free and bureaucracy friendly solution is proposed that will try to automate the processes in the most pain free way possible.

NIST SP 800-128 lists 53 controls in general pertaining to security in an organization whereas, 9 of which solely deal with the configuration management of the society. The 9 controls are specified as follows:

1. CM-1 Configuration Management Policy and Procedures: this control specifies a formal documented process to completely document all the configuration policies with Standard Operating Procedure for implementation.
2. CM-2 Baseline Configuration: the criterion of any configuration system that will be compared to as a benchmark for any deviation of configuration.

3. CM-3 Configuration Change Control: Defining the kinds of modification to be measured under the policy, favoring those changes with cleardeliberation for security impact, and documenting, reviewing and auditing approved changes.
4. Security Impact Analysis: Examining changes to regulateprospective security effectspreceding to change execution
5. Access Restrictions for Change: Defining, documenting, approving, and enforcing physical and logical admissionlimitationaccompanying with variations.
6. Configuration Settings: Developing, recording and employingObligatory configuration settings using security configuration checklists that reflect the most restraining mode coherent with functionalobligations; and recognizingexclusions.
7. Least Functionality: Configuring information systems to provide only indispensableexpertise and expresslyforbidding or confining the practice of functions, ports, rules, and assistance.
8. Information System Component Inventory: Developing, documenting, and maintaining an accurate inventory of information system components that provides the level of granularity necessary for tracking and reporting.
9. Configuration Management Plan: Developing, documenting, and implementing a configuration management plan addressing roles, responsibilities, processes and procedures throughout the system development life cycle.

3.2 Research Methodologies

In this section the research methodologies [38] mean a body of practices, procedures, and rules used those who work in a discipline or engage in an inquiry; a set of workingmethods: the methodol

ogy of genetic studies; a poll marred by faulty methodology.Methodologies can generically classified in two types empirical and theoretical.

3.2.1 Empirical Research Methods:

Empirical research as the name suggest contain research related to practical or observable aspects of the exploration. It contains the jargons like facts, observation, and inference, constructs intermittently. The fact is said to be is a truth which is observed repeatedly. Observation means a systematic data collection approach i.e. researchers using all of their senses to record a particular event. Inference means the conclusion derived from the facts and subsequent observation. Lastly, constructs in empirical research are non-observable deduced outcome that are logical ideas developed by a researcher.

3.2.2 Theoretical Research Methods

Theoretical methods are the most logical forms of research. In this research, all the conclusion are drawn based on abstraction and logic. Mathematics is considered the purest of all the thought forms, is purely based on abstraction and logical derivation which means while deriving mathematical conclusions, all the researcher needs is logical axioms, proofs and conjectures. Conducting research in classical sciences such as mathematics etc. one does not need to have observable data to reach conclusions. An inquisitive mind searching for solutions does not need to do any practical experiments. Other natural sciences such physics and chemistry can have both theoretical and experimental prospects.

3.3 Proposed Method of Study for the Problem

The problem statement defined in the section 1.2 was proposed as follows:

"Developing a coherent solution to expand the functionality of NIST's Scalable Content Automation Protocols with respect to the needs of an academic institution"

In computer science, as it is a relatively new branch of science as compared to the classical sciences whose roots can be found in Greek mythology, the method of research in it has been highly debatable. Since the dawn of computers in the 1940s, the science of computers can be divided into to two distinctive types, first being a classical science since mathematics has played an important part in its development most notable are the works of Shannon, Turing etc. [39] [40]. The mathematical basis of science is dealt with the traditional theoretical mode of research. There is another aspect to the science of computer which is engineering. Engineering tends to solve the problems at hand rather than creating theories about it. Hence the method of researching engineering would be more empirical than practical. The problem at hand is more of an engineering type than mathematical. The solution would be exploring in how to make an existing system better and more functional.The problem this thesis addresses is more of software engineering nature than logical or mathematical as said before. Therefore, according to Per and Höst the research method in this field are yet to defined and grow. The most common forms of research in software engineering are listed below [41]

The problem statement as written before suggests that it is an improvement to an existing system of NIST SCAP and to the processes being run in MCS NUST.

Table 2 Research methods in software engineering

Methodology	Primary Objective	Primary Data	Design
Survey	Descriptive	Quantitative	Fixed
Case Study	Exploratory	Qualitative	Flexible
Experiment	Explanatory	Quantitative	Fixed
Action Research	Improving	Qualitative	Flexible

3.3.1 Action Research Methodology

3.3.1.1 Introduction

Action research is the most practical approaches amongst all while doing the research work. Most of the software solutions are designed after solving real life problems and then distributing results. It works on the principles of identifying a problem and then finding a solution for it. It can be subjective and vague as well since most of the time the organizational politics overcomes the solutions provided but nonetheless, it is most practical and most natural form of research in software engineering [42].

Action research is mostly used in design based scenarios like this one. The following flowchart would better mimic the action research methodology in this one explained in the form of a diagram. [43].

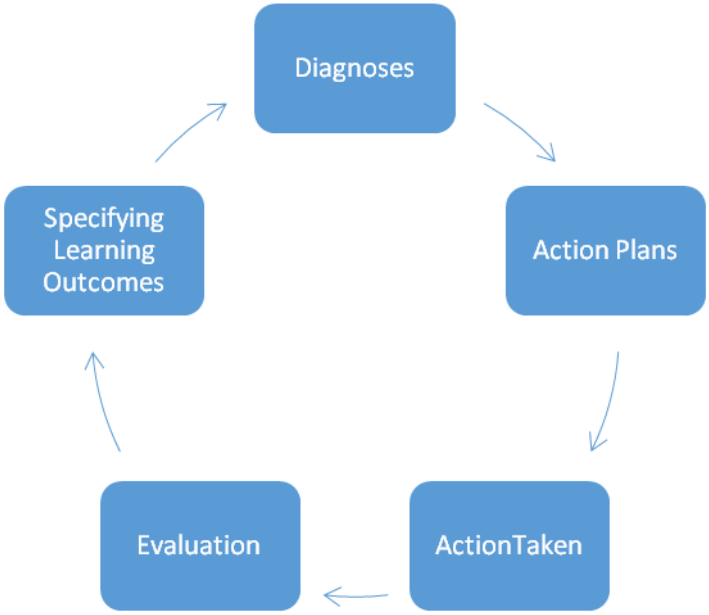

Figure 11 Action research processes

For the better explanation of the action research methodology, following scenario should be in perspective.

Mr. Joe works as a researcher in a lab connected with the industry. He is interested in the deep understanding of how the modeler or developer of the industry use the UML in software implementation and design. His aim is to find out how these practices are used in the industry and how these diagrams are used for cooperativecommunalobjects.

Scenario will now be solved by dividing it into different parts as its cycle is explained in the figure above.

3.3.2 Diagnoses

When Joe started working on the problem, one of his colleagues discussed the “problem” with him about the difficulty they face while integrating software components and predicting the effects of such integration. Joe sees it as an opportunity to work with them to try out ideas from model-driven development, and to study hands on how UML changes the way developers cooperate.

3.3.3 Action Plan

Joe starts a project to work with his colleagues to introduce MDD and to document the events.

3.3.4 Action Taken

The development team uses a series of data collection and extraction techniques like periodic interviews, questionnaires and focus groups.

3.3.5 Evaluation

The data collected from afore-mentioned techniques was used to develop local theories that explain the experiences of the problem owners.

3.3.6 Specifying Learning

The local theories that explain the problem can be generalized with further research.

In the above situation it can be easily comprehended that every time anactual life difficultystands, action research is the way to go. Action research detects a problem, plans the actions to mitigate that problem, applies the action and take observations to foster a theory. This is best suited for critical theory. In action research, the methodology is based on problem solving i.e. the problem to be identified and it should be solved by the end of action research cycle. The accepted answer is also

contemplated as suitable as it is the best tackling that particular problem. Information acquired from the study authorizes specific people or groups and enable a broader change.

3.4 Application of Action Research on Current Scenario

3.4.1.1 Diagnoses

Part of the problem statement requires an example of academic institution. Since from [38], it can be determined that SCAP requires validation for confirming compliance with the specifications. Validation so far, is made commercially by vendors like IBM, MacAfee etc. which is costly and has it limitation.

1. There are certain limitation to the products validated by SCAP, which are:
2. They are not freely available
3. Most of them do not extend the current functionality of SCAP

The document will now explain the research by establishing a problem about the target organization. The solution provided by SCAP does not cater for the academic institutions and only deals with the need of government organizations. Also the solution is not freely available for the users to be more familiarized with the specifications of SCAP. Widespread use of SCAP would only happen if the solution is more open source then closed.

There is now need of a target organization whose processes regarding security can be made more approachable. The organization used here is the Military College of Signals (MCS) by National University of Sciences and Technology (NUST). MCS is strongly affiliated with the Armed Forces before the establishment of NUST. MCS deals with two majors of engineering, electrical and

software Engineering. Electrical engineering has two majors, electronics and telecommunication. Whereas, software also has two majors software and information security. The university also offers post graduate programs of Masters and doctorate of Philosophy (Phd.) in the aforementioned majors. The university campus boasts of history since the establishment of Pakistan in 1947. With its rich history and culture in engineering programs. MCS has served Pakistan with its top-quality engineers. Like any organization, MCS also need to organize the processes involving security. Currently, there is not any formal documentation of security policy available online. NUST has no formal security policy available on its website. This is also the requirement of the institution that the formal security policy is to be documented. However, making and maintaining complete security policy of any organization is not an easy task. For the sake of this document, the author is only going to focus on the configuration policies baseline for the said organization. These policy will determine a benchmark for all the devices attached to the network to be considered as safe or hardened.

Definition of a hardened device also needs to be established before classifying the networks and information systems of MCS. A hardened computer is a system that ensures that latest patches and security configurations are applied to a system so it is resilient against the prevalent computer attacks.

3.4.1.1.1 Current Practices in MCS

Currently, there is a Management Information System (MIS) cell that provides the Information Technology infrastructure that according to the website provides following services:

1. To provide support for doctoral, post-graduate and under-graduate academic research.

2. To vigorously incorporate the use of IT in teaching learning, administration, planning and management.
3. Using technology to enhance student services.
4. Promoting effective and efficient college operations by using e-MS.
5. Upgrading and extending the college IT infrastructure.
6. Assuring comprehensive electronic communication capability for all college constituents [45].

The MIS cell uses Active Directory to manage profiles and security levels in the organization. Active directory is a centralized mechanism to control and manage network administration. Active Directory is Microsoft's execution of directory facilities. It is based on numerous specifications, most essentially LDAP and X.500 (the diagram is based on X.500). In accumulation to agreement with LDAP, AD has supplementary features and compatibility such as the handy incorporation of the directory services to Windows domains and Domain Name Service (DNS). The incorporation of directory services to Windows domains is the crucial to directory capacity to be flexible and stable (domains and scalability will be described below). AD security, verification, and access control are also offered by the assimilation of the domains to the directory. While this tactic operates completely, the incorporation of AD to Windows domains influences the selection of Active Directory services when picking the Windows operating system. The combination of DNS to Windows domains is an aspect that creates the design and execution of Active Directory together complex and intrusive to the prevailing foundation. Prominently, a Windows domain need to be called identically to its DNS domain. The exact DNS name is operated for both the IP address resolution and the Active Directory domain name.

3.4.1.1.2 Features of Active Directory Services

Domain - The central component of logical construction in the Active Directory is the domain, which can stock millions of objects. Objects stored in the domain are measured “stimulating” to the network. “Stimulating” objects are articles the networking group associates want to do their tasks: printers, documents, e-mail addresses, databases, users, and other resources. All network objects occur inside a domain and all domain stocks report merely around objects it encloses. Active Directory is created by one or more domains.

Trees are the physical components that guarantee the scalability of the Active Directory. As every domain is a division (portion of the complete directory), trees permit the categorized construction essential for organizations, much like DNS domain arrangement does for the Internet. Domains in a tree essentially be named equally to their DNS domain names.

Forest - There are instances where more than two domain trees, each characterized by distinct DNS name space, must be involved as one operation. A tree essentially be signified by an adjoining DNS name space and forbid contribution of domains that are not inside its name space. The method for joining one or additional trees is the Forest.

The tasks of a typical active directory can be listed as follows:

1. User data management: Management of group policies, offline folders, synchronization and disk quotas extra.
2. Software Installation and maintenance: software is installed and changes are managed by the active directory.

3. User settings management: customized settings by user are kept the same regardless of the hardware. The user may access different computer but since its login is the same so is the data and settings.
4. Remote software installation: Enabling Windows administrators to install or configure Windows on new or replacement computers without on-site technical support.

3.4.1.1.3 Change Management and Limitations of Active Directory

Change management in Active Directory is a very centralized process. All the computers associated with a specific domain will contain the configurations and it is all dependent on a single domain controller computer. When security is considered, there should always be a decentralized policy, which will shift the dynamics of control and safety to several computers rather than one. In the approach defined by this document, it has been established that the computers should each have their own set of configurations independent of a domain controller entity. This would decentralize the whole system and divide the power individually among computers [40].

Another reason of following this approach would be ensuring, the computers evading the Windows Active directory should be having some sort of configurations management mechanism to thwart prevalent threats in the environment. The group security policy of active directory services has roughly around 1800 policy settings.

3.4.1.1.4 Hardware and Software Establishments in MCS

1. Security policy documents are not available for any level.
2. IP/Domain is single for both faculty and students, no trees and forest are currently in use

3. The faculty and administration offices do not use any proxy server whereas library and student labs do.
4. Domain Name Services are public google, whereas the proxy server is running on UBUNTU
5. MIS cell centrally manages all the IT operations of the university.
6. The labs situation of MCS is as follows
7. DSP lab is an Electronics Engineering Department lab specifically designed for engineering students. It deals with the special equipment which uses following soft wares Matlab and C/C++.
8. CAD is Computer Aided Design Lab which is used by engineering student to solve the design problem. Specialty software like AutoCad is used here.
9. OS (Operating System) is a research lab dedicated to the students of Masters and Doctorate. This lab allows students to experiment and play with the computers however, they like it.
10. IS (Information Security) is the lab used by the information security department. It computers are usually used for demonstrations and training purposes. The lab sometimes does not use the Active Directory Services.
11. Programming Lab I & II are generic labs used by the students of Software Engineering for learning regular course material. The computers in the lab install software specific to the course needs.
12. DB (Database) lab is again maintained for the graduate and post graduate students for research purposes. Students are given a free hand in the installation for experimentations.

13. CASE is a module developed for the combat exams for Army personnel. This lab has the most secure environment and cannot afford to be thwarted by a third party.

3.4.1.2 Action Plans

Action Plan defined here at MCS is to manage and automate the process of configurations management by NIST SCAP. So far the NIST's SCAP have mechanisms to validate the controls not implement them. So, the solution offered would be after checking all the baseline security configurations for a system, to then apply any missing configuration and log the missing configuration to the authorities.

To analyze and gather all the current established procedures at the university and to determine how effective or ineffective those are. After establishing the current situation, the next step would be to determine the solution established by SCAP and to enhancing its practices in a way that the processes are improved. Writing of the security policies and identifying roles with respect to the hierarchy of the environment is also very important. After establishing the policies, application of the policy management software tool must be implemented and its behavior administrated

3.4.1.3 Action Taken

The complete measures taken in this scenario would be explained in a greater detail in chapter number 4. The proposed policies will also be listed there.

3.4.1.4 Evaluation

The complete measures taken in this scenario would be explained in a greater detail in chapter number 5.

3.4.1.5 Specifying Learning

Other observational items will be explored in detail in chapter 6.

4 Proposed Policies

4.1 Introduction

This chapter will focus on writing down the policies tailored to the MCS. It is assumed that the prevalent operating system at the institution would be windows operating system. As mentioned in the details of laboratory systems in chapter 3 section 3.4.1.1.4, most of the educational and technical material used require windows as a medium. The other computers used by research students can contain any software and are not liable for maintenance by institution's administration. The policies will be revolving around the windows security policies accessed by secpol.msc. It is to be noted that it contains too many policies for the administrator to be able to comprehend and maintain by manual labour. The table 3 for policies would be illustrated as below

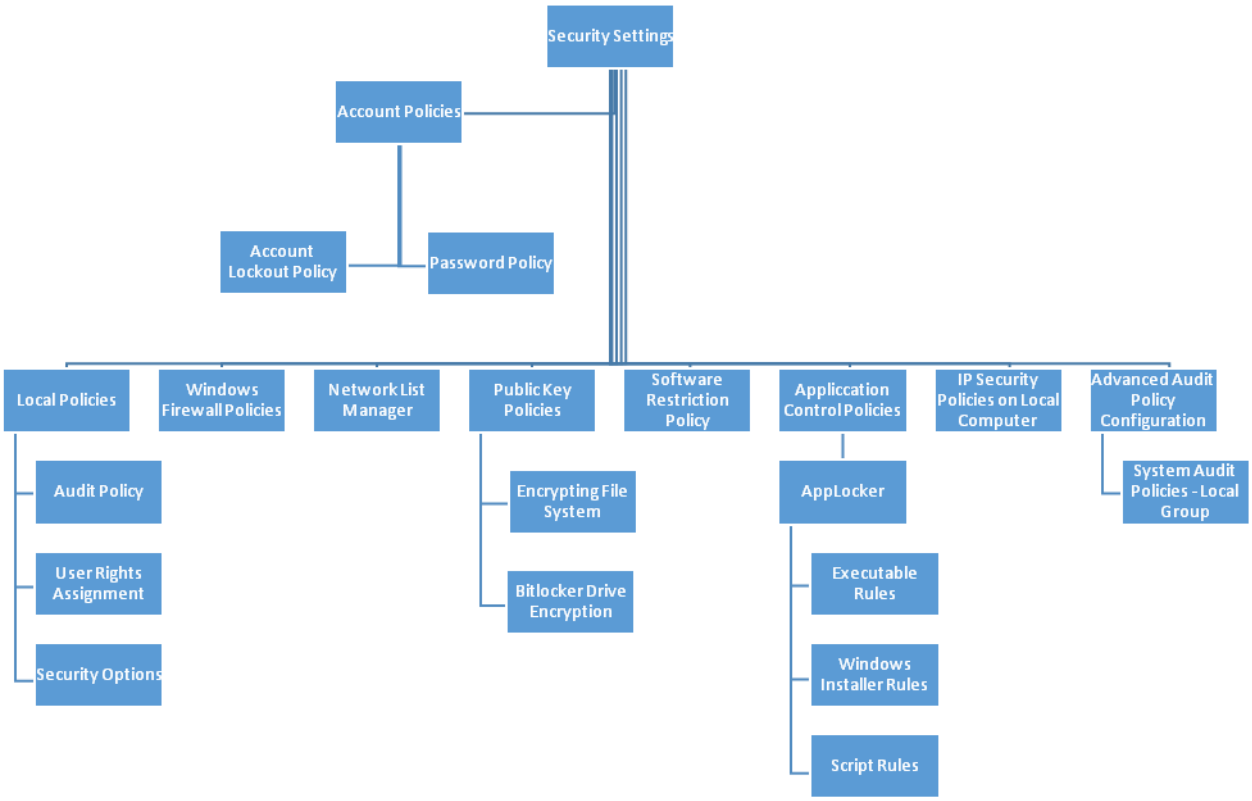

Figure 12 Hierarchy of policies

The above figure is the main hierarchy of the Local Security Policies available on a windows system. The gist of the policies remain the same however, the policies may be updated in subsequent versions of operating system. But the solution is open enough that it will require minimum to low changes required for the upgrade to the operating system. The policies will be divided into three distinct parts

Just like in any organization with Information System infrastructure, the roles are divided into three parts.

1. User – it has the most basic or limited amount of control over the system it is using.
2. Power user – the section of IS with somewhat greater control than the users for usually managing the users.
3. Administrators – this type of user is few and far between. They are the ultimate beholder of power and govern over both users and power user.

Table 3Mapping of policy to roles

Name	Description
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM

Name	Description
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features
Performance Log Users	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer
Performance Monitor Users	Members of this group can access performance counter data locally and remotely
Power Users	Power Users are included for backwards compatibility and possess limited administrative powers
Remote Desktop Users	Members in this group are granted the right to logon remotely
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental or intentional system-wide changes and can run most applications

In the case of this document, the people with most power would be the MIS cell administrators, the power users would be the teachers and users would be the students. The policies defined for each group would be based on the powers bestowed upon them.

Table 4Explanation of Local Security Policy [46] [47]

Policy Name	Administrator	Power User	User
"account lockout duration"	900 seconds	3600 seconds	86400 seconds
"account lockout threshold"	3 attempts	3 attempts	5 attempts
"account lockout reset counter"	900 seconds	3600_seconds	3600_seconds
"password enforce history"	24 passwords	24 password	5 passwords
"password maximum age"	5184000 seconds	5184000 seconds	7776000 seconds
password minimum age	86400 seconds	86400 seconds	172800 seconds
"password minimum length"	12 characters	12 characters	8 characters
"password complexity"	Enabled	Enabled	Enabled
"password reversible encryption"	Disabled	Disabled	Disabled
"accounts administrator account status"	Enabled	Disabled	Disabled
"guest account status"	Disabled	Disabled	Disabled
"limit blank password use"	Enabled	Enabled	Enabled

Policy Name	Administrator	Power User	User
"Adjust Memory Quotas for a process Description"	X	X	X
"Allow Logon Locally"	✓	X	X
"Allow log on through Terminal Services"	✓	✓	X
"Back up files and directories"	✓	X	X
"Bypass Traverse Checking"	✓	X	X
"Change System Time"	X	X	X
"Change the time zone"	X	X	X
"Create a pagefile"	✓	X	X
"Create a Token Object"	X	X	X
"Create Global Objects"	✓	X	X
"Create Permanent Shared Objects"	✓	X	X
"Create Symbolic Links"	✓	X	X
"Debug Programs"	✓	X	X
"Deny Access to this Computer from the Network"	✓	X	X
"Deny Log on as a Batch Job"	X	X	X

Policy Name	Administrator	Power User	User
"Deny Logon as a Service"	X	X	X
"Force shutdown from a Remote System"	X	X	X
"Generate security audits"	X	X	X
"Impersonate a client after authentication"	X	X	X
"Increase a process working set"	X.	X	X
"Increase Scheduling Priority"	X	X	X
"Load and Unload Device Drivers"	✓	X	X
"Lock pages in memory"	✓	X	X
"Log on as a Batch Job"	X	X	X
"Logon as a Service"	X	X	X
"Manage Auditing and Security Log"	✓	X	X
"Modify an Object Label"	✓	X	X
"Modify Firmware Environment Variables"	✓	X	X
"Perform Volume Maintenance Tasks"	✓	X	X

Policy Name	Administrator	Power User	User
"Profile Single Process"	✓	X	X
"Profile System Performance"	✓	X	X
"Remove Computer from docking station"	N/A	N/A	N/A
"Replace a process level token"	X	X	X
"Restore files and directories"	✓	X	X
"Shut down the system"	✓	✓	✓
"Synchronize directory service data"	N/A.	N/A	N/A
"Take ownership of files or other objects"	✓	X	X
"accounts administrator account status "	Disabled	Disabled	Disabled
"guest account status"	Disabled	Disabled	Disabled
"limit blank password use"	Enabled	Enabled	Enabled
"audit use backup restore privilege"	Disabled	Disabled	Disabled
"audit access global system objects"	Disabled	Disabled	Disabled

Policy Name	Administrator	Power User	User
"override audit policy settings"	Enabled	Enabled	Disabled
"shutdown system unable log audits"	Enabled	Disabled	Disabled
"prevent users installing printers"	Disabled	Disabled	Enabled
"restrict cdrom access local users only"	Not restricted	Not restricted	Restricted
"restrict floppy access local users only"	Not restricted	Not restricted	Restricted
"digitally encrypt secure channel data when possible"	Enabled	Enabled	Enabled
"disable machine account password changes"	Disabled	Disabled	Disabled
"maximum machine account password age"	30 days	30 days	30 days
"require strong session key"	Enabled	Enabled	Enabled
"do not display last user name"	Enabled	Enabled	Enabled
"do not require ctrl+alt+del"	Disabled	Disabled	Enabled
"message text users attempting logon"	Any	Any	Any

Policy Name	Administrator	Power User	User
"message title users attempting logon"	Any	Any	Any
"number of previous logons to cache"	1 cached	2 cached	2 cached
"prompt user to change password before expiration"	14 days	14 days	14 days
"smart card removal behavior"	N/A	N/A	N/A
"require domain controller authentication to unlock"	Disabled	Disabled	Disabled
"digitally sign communications client always"	Disabled	Disabled	Disabled
"digitally sign communications client server agrees"	Enabled	Enabled	Enabled
"send unencrypted password to third party SMB servers"	Disabled	Disabled	Disabled
"amount of idle time required before suspending session"	15 minutes	15 minutes	15 minutes
"digitally sign communications server always"	Enabled	Enabled	Enabled

Policy Name	Administrator	Power User	User
"digitally sign communications server client agrees"	Enabled	Enabled	Enabled
"disconnect client when logon hours expire"	Enabled	Enabled	Enabled
"minimum session security NTLM SSP based clients"	Require NTLMv2 and require 128 bit encryption	Require NTLMv2 and require 128 bit encryption	Require NTLMv2 and require 128 bit encryption
"anonymous SID name translation"	Disabled	Disabled	Disabled
"minimum session security NTLM SSP based servers"	Require NTLMv2 and require 128 bit encryption	Require NTLMv2 and require 128 bit encryption	Require NTLMv2 and require 128 bit encryption
"do not allow anonymous enumeration SAM"	Enabled	Enabled	Enabled
"do not allow anonymous enumeration SAM accounts shares"	Enabled	Enabled	Enabled

Policy Name	Administrator	Power User	User
"do not allow storage credentials net passports network authentication"	Enabled	Enabled	Enabled
"let everyone permissions apply to anonymous users"	Disabled	Disabled	Disabled
"restrict anonymous access to named pipes and shares"	Enabled	Enabled	Enabled
"sharing and security model for local accounts"	Classic	Classic	Classic
"do not store lan manager hash value on next password change"	Enabled	Enabled	Enabled
"force logoff when logon hours expire"	Enabled	Enabled	Enabled
"lan manager authentication level"	Send NTLMv2 response only refuse LM and NTLM	Send NTLMv2 response only refuse LM and NTLM	Send NTLMv2 response only refuse LM and NTLM
"ldap client signing requirements"	Negotiate signing	Negotiate signing	Negotiate signing

Policy Name	Administrator	Power User	User
"recovery console allow administrative logon"	Disabled	Disabled	Disabled
"recovery console allow floppy copy access all drives folders"	Disabled	Disabled	Disabled
"digitally encrypt or sign secure channel data always"	Enabled	Enabled	Enabled
"digitally sign secure channel data when possible"	Enabled	Enabled	Enabled
"shutdown allow system shutdown without having logon"	Enabled	Enabled	Enabled
"shutdown clear virtual memory page"	Enabled	Disabled	Disabled
"system cryptography use fips compliant algorithm"	Enabled	Enabled	Enabled
"admin approval mode"	Enabled	Enabled	Enabled
"system objects require case insensitivity"	Disabled	Disabled	Disabled

Policy Name	Administrator	Power User	User
"system objects strengthen default permissions internal system objects"	Enabled	Enabled	Enabled
"behavior elevation prompt administrators"	Prompt for consent	Prompt for consent	Prompt for credentials
"behavior elevation prompt standard users"	Prompt for credentials on the secure desktop	Prompt for credentials on the secure desktop	Prompt for credentials on the secure desktop
"detect application installations prompt elevation"	Enabled	Enabled	Enabled
"only elevate executables signed validated"	Disabled	Disabled	Disabled
"only elevate uiaccess applications"	Enabled	Enabled	Enabled
"run administrators admin approval mode"	Enabled	Enabled	Enabled
"switch secure desktop prompting elevation"	Enabled	Enabled	Enabled
"auto admin logon"	Disabled	Disabled	Disabled

Policy Name	Administrator	Power User	User
"virtualize write failures per user locations"	Enabled	Enabled	Enabled
"IP source routing protection level"	Source routing packets disabled	Source routing packets disabled	Source routing packets disabled
"allow ICMP redirects"	Disabled	Disabled	Disabled
"keep alive time"	300000 seconds	300000 seconds	300000 seconds
"name release requests"	Enabled	Enabled	Enabled
"router discovery"	Disabled	Disabled	Disabled
"safe DLL search mode"	Enabled	Enabled	Enabled
"screen saver grace period"	5 seconds	5 seconds	5 seconds
"TCP max data retransmissions"	Value of 3	Value of 3	Value of 3
"event log threshold warning"	90 percent	90 percent	90 percent
"enable nodefaultexempt ipsec filtering"	Multicastbroadcast isakmprecxp	Multicastbroadcast isakmprecxp	Multicastbroadcast isakmprecxp
"fax service"	Disabled	Disabled	Disabled
"bluetooth support service"	Disabled	Disabled	Disabled
"homegroup listener service"	Disabled	Disabled	Disabled
"homegroup provider service"	Disabled	Disabled	Disabled

Policy Name	Administrator	Power User	User
"media center extender service"	Disabled	Disabled	Disabled
"parental controls service"	Disabled	Disabled	Disabled
"computer account management"	Success failure	Success failure	Success failure
"other account management events"	Success failure	Success failure	Success failure
"security group management"	Success failure	Success failure	Success failure
"user account management"	Success failure	Success failure	Success failure
"process creation"	Success	Success	Success
"logoff"	Success	Success	Success
"logon"	Success failure	Success failure	Success failure
"special logon"	Success	Success	Success
"file system"	Failure	Failure	Failure
"registry"	Failure	Failure	Failure
"policy change audit"	Success failure	Success failure	Success failure
"authentication policy change"	Success	Success	Success
"sensitive privilege use"	Success failure	Success failure	Success failure
"ipsec driver"	Success failure	Success failure	Success failure
"security state change "	Success failure	Success failure	Success failure
"security system extension"	Success failure	Success failure	Success failure

Policy Name	Administrator	Power User	User
"system integrity"	Success failure	Success failure	Success failure
"turn on mapper io lltdio driver"	Disabled	Disabled	Disabled
"turn on responder rspndr driver"	Disabled	Disabled	Disabled
"turn off microsoft peer to peer networking services"	Enabled	Enabled	Enabled
"prohibit installation network bridge"	Enabled	Enabled	Enabled
"require domain users to elevate when setting a networks location"	Enabled	Enabled	Enabled
"route all traffic through the internal network"	Enabled state	Enabled	Enabled
"6to4 state"	Disabled	Disabled	Disabled
"isatap state"	Disabled	Disabled	Disabled
"teredo state"	Disabled	Disabled	Disabled
"ip https state"	Disabled	Disabled	Disabled
"ip https url "	Any	Any	Any
"configuration of wireless settings using windows connect now"	Disabled	Disabled	Disabled

Policy Name	Administrator	Power User	User
'prohibit access of the windows connect now wizards"	Enabled	Enabled	Enabled
"extend point and print connection to search windows update and use alternate connection if needed"	Disabled	Disabled	Disabled
"allow remote access to the pnp interface"	Disabled	Disabled	Disabled
"do not create system restore point when new device driver installed"	Disabled	Disabled	Disabled
"do not send windows error report when generic driver is installed on device "	Enabled	Enabled	Enabled
"prevent device metadata retrieval from the internet"	Enabled	Enabled	Enabled
"specify search order for device driver source locations"	Do not search windows update	Do not search windows update	Do not search windows update
Policy Name	Administrator	Power User	User

"registry policy processing"	Enabled:nogpolistchanges	Enabled:nogpolistchanges	Enabled:nogpolistchanges
"no background policy change"	Disabled	Disabled	Disabled
"no gpo list changes"	Enabled	Enabled	Enabled
"turn off downloading of print drivers over http"	Enabled	Enabled	Enabled
"turn off event views events asp links"	Disabled	Disabled	Disabled
"turn off printing over http"	Enabled	Enabled	Enabled
"turn off internet connection wizard if url connection is referring to Microsoft"	Enabled	Enabled	Enabled
"turn off internet download for web publishing and online ordering wizards"	Enabled	Enabled	Enabled
"turn off internet file association service"	Enabled	Enabled	Enabled
Policy Name	Administrator	Power User	User

"turn off registration if url connection is referring to Microsoft"	Enabled	Enabled	Enabled
"turn off search companion content file updates"	Enabled	Enabled	Enabled
"turn off the order prints picture task"	Enabled	Enabled	Enabled
"turn off the publish to web task for files and folders"	Enabled	Enabled	Enabled
"turn off the windows messenger customer experience improvement program"	Enabled	Enabled	Enabled
"turn off windows error reporting"	Enabled	Enabled	Enabled
"turn off handwriting recognition error reporting"	Enabled	Enabled	Enabled
"turn off handwriting personalization data sharing"	Enabled	Enabled	Enabled
"always use classic logon"	Enabled	Enabled	Enabled
"Do not process the run once list"	Enabled	Enabled	Enabled
Policy Name	Administrator	Power User	User

"require a password when a computer wakes on battery"	Enabled	Enabled	Enabled
"require a password when a computer wakes plugged"	Enabled	Enabled	Enabled
"offer remote assistance"	Disabled	Disabled	Disabled
"solicited remote assistance"	Disabled	Disabled	Disabled
"turn on session logging"	Enabled	Enabled	Enabled
"restrictions for unauthenticated rpc clients"	Enabled:authenticated	Enabled:authenticated	Enabled:authenticated
"rpc endpoint mapper client authentication"	Enabled	Enabled	Enabled
"enable disable perftrack"	Disabled	Disabled	Disabled
"configure windows ntp client"	Any	Any	Any
"microsoft support diagnostic tool turn on msdt interactive communication with support provider"	Disabled	Disabled	Disabled
Policy Name	Administrator	Power User	User

"troubleshooting allow user to access online troubleshooting content on Microsoft servers from the troubleshooting control pane"	Disabled	Disabled	Disabled
"turn off program inventory"	Enabled	Enabled	Enabled
"turn off autoplay for non-volume devices"	Enabled	Enabled	Enabled
"default behavior for autorun"	Do not execute autorun commands	Do not execute autorun commands	Do not execute autorun commands
"turn off autoplay"	All drives	All drives	All drives
"enumerate administrator accounts on elevation"	Disabled	Disabled	Disabled
"digital locker"	Enabled	Enabled	Enabled
"disable unpacking installation gadgets not digitally signed"	Enabled	Enabled	Enabled
"turn off user installed windows sidebar gadgets"	Enabled	Enabled	Enabled
"maximum application log size"	Enabled:32768 kb	Enabled:32768 kb	Enabled:32768 kb
Policy Name	Administrator	Power User	User

"maximum security log size "	Enabled:81920 kb	Enabled:81920 kb	Enabled:81920 kb
"maximum setup log size"	Enabled:32768 kb	Enabled:32768 kb	Enabled:32768 kb
"maximum system log size"	Enabled:32768 kb	Enabled:32768 kb	Enabled:32768 kb
"turn off downloading of game information"	Enabled	Enabled	Enabled
"turn off game updates"	Enabled	Enabled	Enabled
"prevent the computer from joining a homegroup"	Enabled	Enabled	Enabled
"disable remote desktop sharing"	Enabled	Enabled	Enabled
"do not allow passwords to be saved"	Enabled	Enabled	Enabled
"allow users to connect remotely using remote desktop services"	Disabled	Disabled	Disabled
"set client connection encryption level"	High	High	High
"always prompt client for password upon connection"	Enabled	Enabled	Enabled
Policy Name	Administrator	Power User	User

"set timelimit for disconnected sessions"	60 seconds	60 seconds	60 seconds
"set timelimit for active but idle terminal services sessions"	900 seconds	900 seconds	900 seconds
"do not delete temp folders upon exit"	Disabled	Disabled	Disabled
"do not use temporary folders per session"	Disabled	Disabled	Disabled
"turn off downloading of enclosures"	Enabled	Enabled	Enabled
"allow indexing of encrypted files"	Disabled	Disabled	Disabled
"prevent indexing uncached exchange folders"	Disabled	Disabled	Disabled
"prevent windows anytime upgrade from running"	Enabled	Enabled	Enabled
"configure ms spynet reporting"	Disabled	Disabled	Disabled
"disable logging"	Disabled	Disabled	Disabled
"disable windows error reporting"	Enabled	Enabled	Enabled
"display error notification"	Disabled	Disabled	Disabled
Policy Name	Administrator	Power User	User

"do not send additional data"	Enabled	Enabled	Enabled
"turn off heap termination corruption"	Disabled	Disabled	Disabled
"turn off shell protocol protected mode"	Disabled	Disabled	Disabled
"turn off data execution prevention for explorer"	Disabled	Disabled	Disabled
"disable ie security prompt windows installer scripts "	Disabled	Disabled	Disabled
"enable user control over installs"	Disabled	Disabled	Disabled
"prohibit non administrators install signed updates"	Enabled	Enabled	Enabled
"report logon server not available during user logon"	Enabled	Enabled	Enabled
"turn off the communities features"	Enabled	Enabled	Enabled
"windows mail application manual launch permitted"	Denied	Denied	Denied
Policy Name	Administrator	Power User	User

"prevent windows media drm internet access"	Enabled	Enabled	Enabled
"do not show first use dialog boxes"	Enabled	Enabled	Enabled
"prevent automatic updates"	Enabled	Enabled	Enabled
"no automatic updates"	Disabled	Disabled	Disabled
"reschedule automatic updates scheduled installations"	Enabled	Enabled	Enabled
"no auto restart with logged on users for scheduled automatic updates installations"	Disabled	Disabled	Disabled
"do not display install updates and shut down option in shut down windows dialog box"	Disabled	Disabled	Disabled
"microsoft network server server spn target name validation level"	Accept if provided by client	Accept if provided by client	Accept if provided by client
"Network security Allow Local System to use computer identity for NTLM "	Enabled	Enabled	Enabled
Policy Name	Administrator	Power User	User

Network security Allow LocalSystem NULL session fallback	Disabled	Disabled	Disabled
Network Security Allow PKU2U authentication requests to this computer to use online identities	Disabled	Disabled	Disabled
"Network Security Configure encryption types allowed for Kerberos"	RC4 HMAC MD5 AES128 HMAC SHA1 AES256 HMAC SHA1 Future Encryption Types	RC4 HMAC MD5 AES128 HMAC SHA1 AES256 HMAC SHA1 Future Encryption Types	RC4 HMAC MD5 AES128 HMAC SHA1 AES256 HMAC SHA1 Future Encryption Types
"User Account Control Allow UIAccess applications to prompt for elevation without using the secure desktop "	Disabled	Disabled	Disabled
"Access this computer from the network"	✓	X	X

5 Implementation and testing

5.1 Introduction

In this section first the technique is to discuss the implementation of the automation process. In the automation process, the XML files are kept encrypted as a data source. After the decryption of the xml files, the profiles selected by user at the time of installation is chosen and a number of different automating techniques is applied. Not all the values are present in the registry or hidden from the user for security purposes. For this purpose the templates of security configurations are made and applied. After application of configuration the system installs itself in the autorun directory and resides in the main memory. Whenever accidental or intentional change of configurations is made, the system automatically shift its configuration back to the original form at the next boot.

5.2 Specification, Architecture and Design

5.2.1 Specification

All of the implementation is done on .Net technologies. The program is developed in C# and the data source used is XML. The program is using various libraries of C# important of those are as following:

1. System.Linq: this namespace rovides classes and interfaces that support queries that use Language-Integrated Query (LINQ). s a Microsoft .NET Framework component that adds native data querying capabilities to .NET languages
2. System.IO: namespace contains types that allow reading and writing to files and data streams, and types that provide basic file and directory support.

3. Microsoft.Win32: the Microsoft.Win32 namespace provides two types of classes: those that handle events raised by the operating system and those that manipulate the system
4. Registry.System.Security: the System.Security namespace provides the underlying structure of the common language runtime security system, including base classes for permissions.

5.2.2 Architecture

The architecture is based on .NET framework 4.0. It is primarily chosen because it fulfills the requirement of the target system being windows 7.

5.2.3 Design

The design can be easily divided roughly into four parts:

1. Management of the data source:

   The management of data source is conducted by keeping xml files for the exchange of information. Since exchange of information should be platform independent. Hence, the required medium of data source is XML. This allows us to be able to standardize and transfer information easily. For the sake of security the XML files used here are encrypted.

2. Usage of Template files:

   After extracting required information from the data source. The program is designed to divide the configurations according to the type managed by the operating system. The password and account policy is managed by the template files. There is no exposure of these setting through program due to security reasons. Hence template file with the values specified in the data source is created.

3. Making registry values

Most of the registry key values pertaining to the group policy setting are not created until and unless they are activated. This program converts all required and important group policies into the specific registry values they are supposed to be.

4. Using LSA wrapper class

Using a local security authority class (LSA) to perform rights granting methods. The program uses a specific class wrapped by managed C# code to grant various rights throughout the program. The rights are role based and are divided into three types: user, power user and administrators.

5. Installation files

The completed program is then compiled in installation files and are installed as such that the program is enforcing properties at each boot up of the operatingsystem.

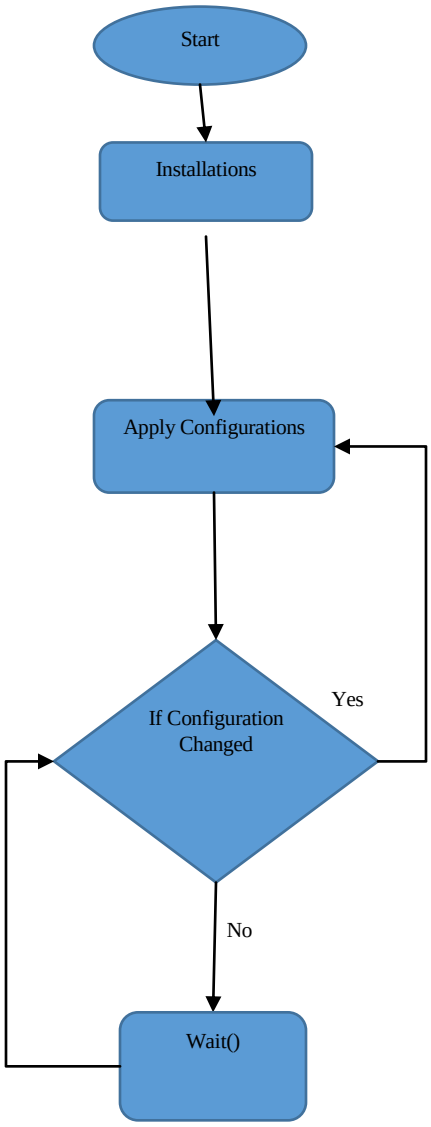

Figure 14 Flow of application (generic)

5.3 Testing

This section has been divided into two parts before and after scenario. In this document the measurement of baseline security configuration is taken by the Microsoft internal software baseline security analyzer. The version used for testing this would be windows 7 and the tools version would

be 2.3. The following is the before shot of security analyzer, which shows that the security configurations are not yet implemented.

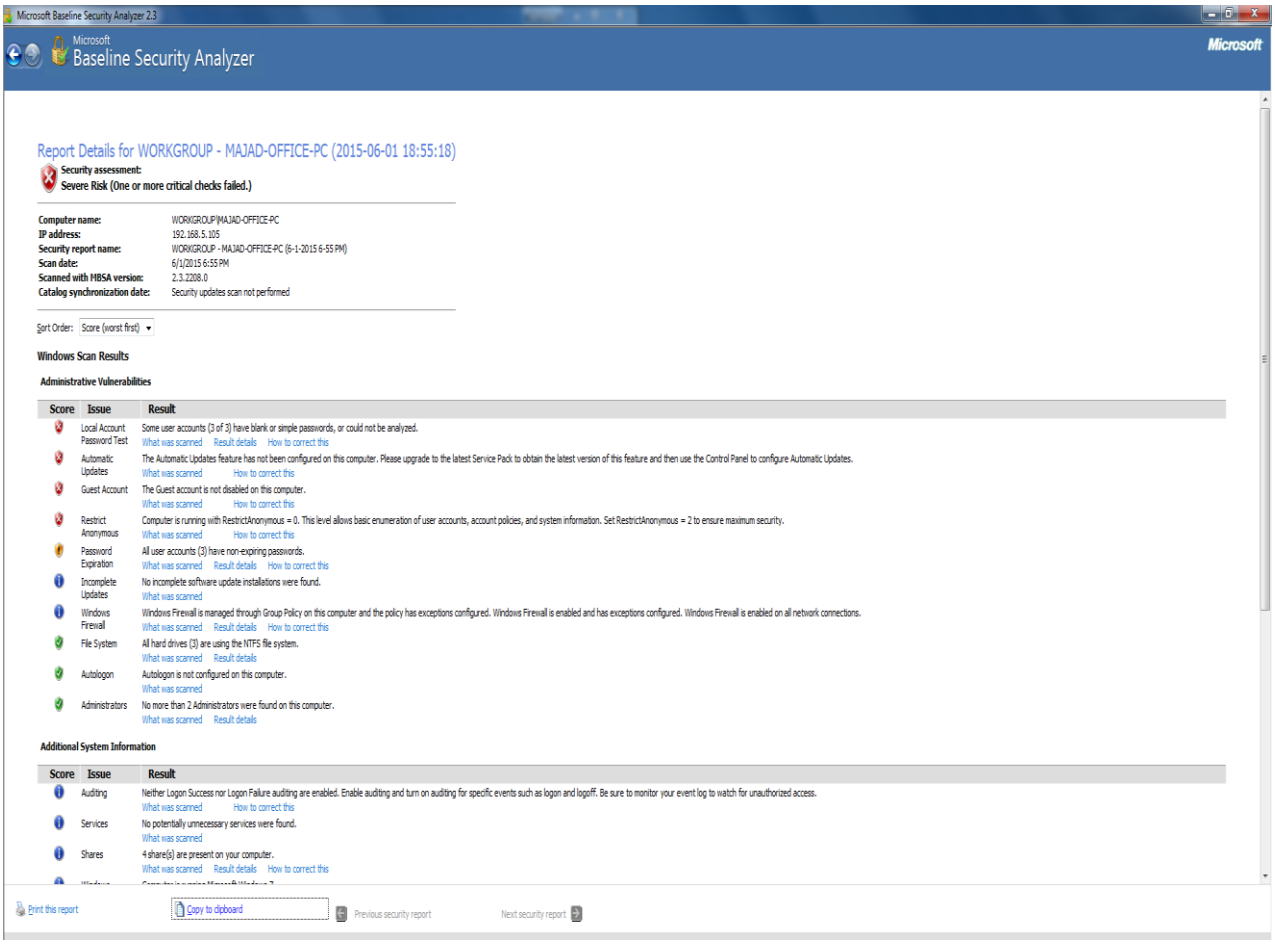

Figure 15 before application of policies

In this it can be easily seen that few of the controls are not applied.

And the after figure is as below:

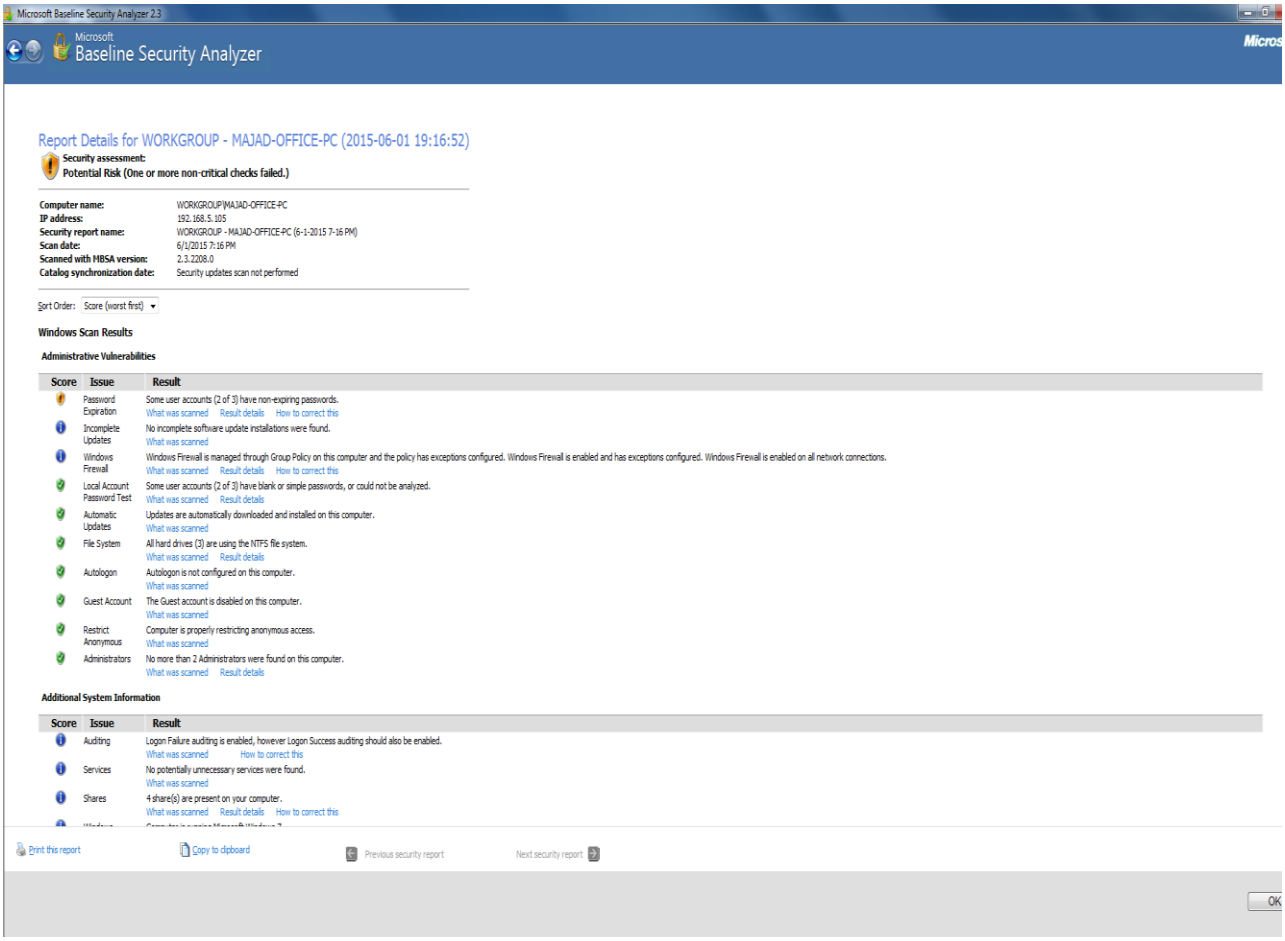

Figure 16 after application of policies

5.4 Conclusion

It can be noted that running the program fulfils the need of automatic security configuration. The tool itself is provided in the CD with this document. The reader can install and use it for itself.

6 Conclusion

6.1 Introduction

The automated configuration for computers is not yet developed by Microsoft. The tools provided by Microsoft are too cumbersome and difficult to use. In this document a new approach towards holistic configuration management has been applied. The tools which are accredited by SCAP are only scanners and that rate a system against a set of configurations baselines. They do not cater for the rapid and unexpected configuration management that should be a part of an agile and forward thinking organization.

6.2 Objective Achieved

1. Study and understanding of SCAP. Understanding of SCAP is an absolute must in this case. Since the thesis is trying to document how the configuration management can be controlled in a specific light. Hence, it needs to studied carefully and thought upon.

2. To identify the workstations/servers information in the academic organization and classify it according to the security severity needs. The complete idea of the workstations in any organization will help in better understanding the complex layers of its hierarchy and its relations with the role of that organization. This is a vital step in providing an efficient and effective tool for the configuration management automation.

3. To develop and write specific security configuration management policies with respect to standards provided by SCAP (Secure Content Automation Protocol). SCAP policies are written in XML and they only quantify the score of a system related to the baseline configurations. This thesis addressed on solving and applying the baseline configurations in an effective manner. So that a system is protected rather than rated against a set of configurations.

4. To implement a tool like functionality to accept the SCAP defined policies and collect workstations information about a system being properly configured or not. This tool accept an xml document as its data source and applies the xml document for effective and timely configurations management.

6.3 Limitation

The limitations are as follows:

1. The system was developed for a specific type of windows version. For example the tool was created for the Windows 7 but it can easily be ported to the current version Windows 10 with minimum changes. As the reader knows there will not be any major upgrades after the version 10 rather free updates. So the tool developed is forward compatible.
2. The system only works for configuration application not malware or vulnerability mitigation. This solution can only prevent a malware risk for any organization as explained in aforementioned chapter but not in the roles of antivirus software.
3. The system designed for a specific type of organization as part of active research. It is not meant to be sold commercially and would require major testing if rolling out as a product.

6.4 Future Directions

The future directions could be as follows;

1. Development of server and domain controller policies in addition to client workstations. These would help integrate this as an end to end solution rather than working as independently. There should also be a mechanism in which the change in configurations should be logged.
2. Integration of data logged by desktop in program for OSIEM (Open Source Threat Management) for deeper analysis of the organization. It would help in understanding how a malware behaves with respect to configurations management. Which settings are disabled or enabled whenever an organization is under threat.
3. Development of SCAP based configuration rules testing tools. These tool or scanners should be free to use, so that anybody can use and integrate them for effective security.

6.5 Concluding Remarks

This document provides a new approach and decentralized approach to configuration management. Poorly designed configurations of the system can be the utmost weakness of any system that can be easily mitigated. The Microsoft and SCAP has limited functionality and increased complexity which was targeted in this document.

Appendix

Table 5 Explanation of Windows Policy [46][47]

Name	Description
"Account lockout duration"	This policy determines how long a user has to wait before he/she can access his/her account again. This is typically set to a low but considerable value. For example a genuine user that is locked out has to wait only 15 minutes instead of asking a manager each instance to undo the account lock. If there is an attacker it can definitely not access with brute forcing the password.
"Account lockout threshold"	This defines the maximum number of unsuccessful efforts that can be allowed by the operating system before locking the account.
"Account lockout reset"	It is the time period associated with the lockout threshold value. If for example, threshold can only have 5 attempts and duration is 15 minutes then the account will probably lock out. If the attempts are 5 but time period is 20 then probably not.
"Enforce password history"	This setting, if enabled forces the system to remember passwords. Which is very important whenever it comes to attacks. Passwords should not be the same and repeated as it weakens the system.
"Minimum password length"	It denote the minimum length of password in characters.

"Minimum password age"	This needsoperators to hang on to a particularinterval of datesbefore changing their password again.
"Maximum password age"	This determines the time period to which the password would remain valid. It is also very important since password should be changed regularly to avoid the threat of attackers guessing the password.
"Password must meet complexity requirements"	This makes user to use special characters which can enforce greater security since the computer then cannot be prone to dictionary attacks.
"Store passwords using reversible encryption"	This setting should not be used in any way since it allows the password to be decrypted by the attacker. It should not be enabled at any cost.
"Access this computer from the network"	This right should be verified that it is assigned correctly.
"Act as part of the operating system"	This right should be verified that it is assigned correctly.
"Adjust memory quotas for a process"	This right should be verified that it is assigned correctly.
"Allow log on locally"	This right should be verified that it is assigned correctly.
"Allow log on through remote desktop services"	This right should be verified that it is assigned correctly.
"Back up files and directories"	This right should be verified that it is assigned correctly.

”Bypass traverse checking”	This right should be verified that it is assigned correctly.
”Change the system time”	This right should be verified that it is assigned correctly.
”Change the time zone”	This right should be verified that it is assigned correctly.
”Create a pagefile”	This right should be verified that it is assigned correctly.
”Create a token object”	This right should be verified that it is assigned correctly.
”Create global objects”	This right should be verified that it is assigned correctly.
”Create permanent shared objects”	This right should be verified that it is assigned correctly.
”Create symbolic links”	This right should be verified that it is assigned correctly.
”Debug programs”	This right should be verified that it is assigned correctly.
”Deny access this computer from the network”	This right should be verified that it is assigned correctly.
”Deny log on as a batch job”	This right should be verified that it is assigned correctly.
”Deny log on as a service”	This right should be verified that it is assigned correctly.
”Deny log on locally”	This right should be verified that it is assigned correctly.
”Deny log on through remote desktop services”	This right should be verified that it is assigned correctly.
”Generate security audits”	This right should be verified that it is assigned correctly.
”Force shutdown from a remote system”	This right should be verified that it is assigned correctly.

"Impersonate a client after authentication"	This right should be verified that it is assigned correctly.
"Increase a process working set"	This right should be verified that it is assigned correctly.
"Increase scheduling priority"	This right should be verified that it is assigned correctly.
"Load and unload device drivers"	This right should be verified that it is assigned correctly.
"Lock pages in memory"	This right should be verified that it is assigned correctly.
"Log on as a batch job"	This right should be verified that it is assigned correctly.
"Log on as a service"	This right should be verified that it is assigned correctly.
"Manage auditing and security log"	This right should be verified that it is assigned correctly.
"Modify an object label"	This right should be verified that it is assigned correctly.
"Modify firmware environment variables"	This right should be verified that it is assigned correctly.
"Profile single process"	This right should be verified that it is assigned correctly.
"Perform volume maintenance tasks"	This right should be verified that it is assigned correctly.
"Profile system performance"	This right should be verified that it is assigned correctly.
"Remove computer from	This right should be verified that it is assigned correctly.

docking station"	
"Replace a process level token"	This right should be verified that it is assigned correctly.
"Restore files and directories"	This right should be verified that it is assigned correctly.
"Shut down the system"	This right should be verified that it is assigned correctly.
"Take ownership of files or other objects"	This right should be verified that it is assigned correctly.
"Accounts administrator account status"	This right should be verified that it is assigned correctly.
"Accounts guest account status"	The threat of vulnerability increases if the built-in guest account is enabled. It should be disabled at all costs.
"Accounts limit local account use of blank passwords to console logon only"	It should be enabled since it allows the attackers and malware from gaining remote access through blank passwords.
"Accounts rename administrator account"	It may frustrate a potential attacker from finding out the administrator accounts which should be done on high risk computers.
"Accounts rename guest account"	It may also annoy and prevent a potential attacker when trying to locate a guest account.
"Audit the access of global system objects"	When this is enabled, it controls the security access control list for the system objects such as events, mutexes, semaphores and DOS devices.

"Audit the use of backup and restore privilege"	It controls the accountability for the use of all user privileges, including Backup and Restore.
"Audit force policy subcategory settings to override audit policy category settings"	It allows a system to override the audity policy category with audit policy subcategory settings.
"Devices prevent users from installing printer drivers"	It allows which users can install a printer driver for the network printer and which cannot.
"Devices restrict cdrom access to locally logged on users"	It should be enabled since by default some processes in the background allows a CD ROM to be accessed by the network in which the computer is operating.
"Devices restrict floppy access to locally logged on users"	It should be enabled since by default some processes in the background allows a floppy disk to be accessed by the network in which the computer is operating.
"Domain member digitally encrypt or sign secure channel data always"	By enabling this policy the outgoing traffic on secure channel should always be encrypted.
"Domain member digitally encrypt secure channel data when possible"	This setting would encrypt most of the data but not all of it if it is enabled.
"Domain member digitally	It ensure all outgoing traffic on secure channel is signed.

sign secure channel data when possible"	
"Domain member disable machine account password changes"	This policy should be enabled since it allows a new password for the computer account to be generated every week.
"Domain member maximum machine account password age"	This control set the maximum password of a machine account. It is not recommended that the password should be set for more than 30 days ensuring change of passwords every month.
"Domain member require strong windows 2000 or later session key"	This controls set the obligatoryforte of a session key.
"Interactive logon do not display last user name"	This control regulates the last name of the user to be displayed or not during logon.
"Interactive logon do not require ctrl+ alt+del"	It should be enabled since it determines that the password sent to the windows after logon are sent to the windows only and not any malicious user waiting to receive the windows password.
"Interactive logon message text for users attempting to log on"	Nil for the case in point.
"Interactive logon message title for users attempting to	Nil for the case in point.

log on"	
"Interactive logon number of previous logons to cache in case domain controller is unavailable"	This should be disabled in all accounts since it allows an attacker to isolate a system and then use a password cracking software to try and gain access to the domain.
"Interactive logon prompt user to change password before expiration"	This should be enabled since it gives the user the deadline that the system password is about to expire and user has time to create a adequately robust password.
"Interactive logon require domain controller authentication to unlock workstation"	This should be enabled for a domain oriented system since it always ensures that the credential are passed to the domain controller for authentication for unlocking purposes.
"Interactive logon smart card removal behavior"	It is applicable only if the smart card is installed which is not the case in our problem area.
"Microsoft network client digitally sign communications always"	This settingvalidate that the customerstrategy is fixed to foreverdigitally sign packets.
"Microsoft network client digitally sign communications if server agrees"	This settingvalidate that the client policy is fixed to digitally sign packets if the server agrees.
"Microsoft network client	Plain text passwords sent to the SMB server decrease the complete

send unencrypted password to third party smb servers"	safety of the location. There should be a way to support the encoded password verification.
"Microsoft network server amount of idle time required before suspending session"	This setting should be used when a computer disconnects the stopped SMB session. If the session is recommenced the validation should be automatically reestablished.
"Microsoft network server digitally sign communications always"	The setting determines the packets are always digitally signed.
"Microsoft network server digitally sign communications if client agrees"	The setting should only sign packets when the client agrees.
"Microsoft network server disconnect clients when logons expire"	The system users should not be allowed to continue registered in the network after their session has passed the required length. In this case if the session is still there an attacker may be lurking in the shade to attack and the hijack the session.
"Network access allow anonymous sid name translation"	It decides if an unidentified user can appeal SID information to get a username or vice versa.
"Network access do not allow anonymous enumeration of sam accounts"	If the following check is disabled, it permits the unidentified users to list all the account names hence a chart of possible purpose to strike.

"Network access do not allow anonymous enumeration of sam accounts and shares"	If the following check is disabled, it permits the unidentified users to list all the account names and all shared resources hence a chart of possible purpose to strike.
"Network access do not allow storage of passwords and credentials for network authentication"	This enables that the credentials should not ever be kept on local machines for account concedes.
"network access let everyone permissions apply to anonymous user"	This setting if enabled allows anonymous users to have the same rights and permission as the default built-in everyone group. It should be avoided at all costs.
"network access named pipes that can be accessed anonymously"	This check determines which of the pipes the anonymous users may enter.
"network access remotely accessible registry paths"	System\CurrentControlSet\Control\ProductOptions; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion
"network access remotely accessible registry paths and sub paths"	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog,

	Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog
"network access restrict anonymous access to named pipes and shares"	This settingestablishesifnamelessentry is limited to christened pipes and shares.
"network access shares that can be accessed anonymously"	It is advised that it should be kept as the default setting.
"network access sharing and security model for local accounts"	The classic model is suggested.
"network security do not store lanmanager hash on	The LAN manager hash is a weak encoding process and hence not recommended.

next password change"	
"network security force logoff when logon hours expire"	When there are logon hours set for the user, this setting should be forced for the users to be forced to log off.
"network security lanmanager authentication level"	This setting defines the security authentication level. It is recommended that the level should be set to Send NTLMv2 response only or refuse LM and NTLM.
"network security ldap client signing requirements"	This setting should be set to requiring sign for providing the insurance of consented verification of communications channel.
"network security minimum session security for ntlm ssp based including secure rpc clients"	This check controls and monitors the features of communications established by a workstation.
"network security minimum session security for ntlm ssp based including secure rpc servers"	This feature determines communication services established by the workstation to other workstations.
"recovery console allow automatic administrative	This setting should generally be disabled.

logon"	
"recovery console allow floppy copy and access to all drives and folders"	This check is enabled by default and should be disabled for security purposes.
"shutdown allow system to be shut down without having to log on"	For such settings where abrupt reboots may cause a problem, system should require a logon before reboot.
"shutdown clear virtual memory page file"	This setting ensures that the computer is wiped down of all the data prior to shut down even the hibernations files. This prevents security tampering.
"System cryptography use fips compliant algorithms for encryption hashing and signing"	It is recommended to use FIPS compliant algorithms.
"System objects require case insensitivity for non-windows subsystems"	This setting is only applicable in Unix and Linux paradigms. It should be ignored when the system is communicating to windows systems only.
"system objects strengthen default permissions on internal system objects"	If this is enabled it allows the Access Control List to other non-administrative organizational procedures to inquire inner system object but not adjust them.
"Microsoft network server	It determines the level of authentication a computer has with its

spn target name validation level"	shared folders or printers.
"Network security Allow Local System to use computer identity for NTLM"	It allows services executing as Local system to utilize the system individuality when discussing NTLM validation
"Network security Allow Local System NULL session fallback"	This systemestablishmentpermits the workstation to revert on a NULL session.
"Network Security Allow PKU2U authentication requests to this computer to use online identities"	It allows a system to negotiate the method of authentication.
"Network Security Configure encryption types allowed for Kerberos"	It permits a system to specify the different types of encryption for Kerberos authentication
"User Account Control Allow UIAccess applications to prompt for elevation without using the secure desktop"	If this is enabled, the level of security is lowered but remote desktop is made available. Should be done on limited very emergency cases.
"bluetooth support service"	Should be enabled if faxes are used in the system.

"homegroup listener service"	If this is not enabled it will make system error prone in a homegroup environment.
"homegroup provider service"	The services is recommended to keep running for good flow of operations.
"media center extender service"	It helps media center to connect and locate to the system.
"parental controls service"	Provided for backward compatibility only.
"credential validation"	It provides the results for test of authentication on authorizations sent for a logon account appeal.
"computer account management"	Audit policy of each event report for a computer account, when computer is created, changed etc.
"other account management events"	This audit ruletellsextra account organizationprocedures.
"security group management"	It tells of the audit policy reports of security group management.
"user account management"	It tells of the audit policy reports of user account management.
"process creation"	Report of the creation of process and the name of the program or user

	who created it.
"Logoff"	Reporting when user logs off from a system
"Logon"	Reporting when user logs in the system.
"Special logon"	Reporting a use of a special logon.
"File system"	Whenever file system is accessed. It should be done by in a manner matching the SACLs and everything should be audited.
"Registry"	Whenever registry is accessed. It should be done in a manner matching the SACLs and everything should be documented.
"Audit policy change"	Reporting change in audit policy.
"Authentication policy change"	Reporting change in authentication policy.
"Sensitive privilege use"	Reporting whenever a user is using a sensitive privilege.
"Ipsec driver"	Audit policy of the IPsec driver of windows.
"Security state changes"	Audit policy of security state changes.
"Security system extension"	It focuses on loading extension code for example authentication packages by the security system.
"System integrity"	Reporting violation of integrity in the subsystem of security.
"Turn on mapper io lltdio	It switches on Mapper I/O network protocol driver. It allows a

driver"	computer to discover network topology where it is connected.
"Turn on responder rspndr driver"	It allows a computer to participate in requests to Link Layer Network topology discovery. It can be discovered and located on the network.
"Turn off Microsoft peer to peer networking services"	It allows Microsoft peer to peer networking services to be turned off and all dependent programs to end performing.
"prohibit installation and configuration of network bridge on your dns domain network"	This setting should be properly configured.
"require domain users to elevate when setting a networks location"	Users should be elevating to higher rights when they are setting their network location.
"route all traffic through the internal network"	
"6to4 state"	It should allow this policy to properly configure.
"Isatap state"	It should allow this policy to properly configure.
"Teredo state"	It should allow this policy to properly configure.
"ip https"	It should allow this policy to properly configure.

"configuration of wireless settings using windows connect now"	The configuration should be done properly.
"prohibit access to the windows connect now wizards"	It should allow this policy to properly configure.
"extend point and print connection to search windows update and use alternate connection if needed"	It allows to control the process of managing client computer searching for Point and printer drivers.
"allow remote access to the pnp interface"	Remotely performed admittance to pnp interface should be allowed.
"do not send a windows error report when a generic driver is installed on a device"	Prohibit sending a windows error reporting whenever a driver of generic variety is installed.
"prevent creation of a system restore point during device activity that would normally prompt creation of a restore	Creation of a system restore point whenever any driver is installed.

point"	
"prevent device metadata retrieval from the internet"	It prohibits from downloading meta data of media files from the internet.
"Specify search order for device driver source locations"	Determining the order in which the operating system locates and finds secure location for storing device drivers.
"Registry policy processing"	Policy processing in administrative templates.
"Turn off downloading of print drivers over http"	Switching off the downloading of the print drivers over world wide web protocol http.
"turn off event viewer events asp links"	Turning off event viewer.asp links.
"turn off handwriting personalization data sharing"	To turn off the handwriting of personalized sharing of data.
"turn off handwriting recognition error reporting"	Error reporting of the handwriting recognition should be turned off.
"turn off internet connection wizard if url connection is referring to microsoft.com"	Switching of the universal resource locator connection of the wizard if it takes you to Microsoft.com
"turn off internet download for web publishing and online ordering wizards"	It is advised to disable the setting aforementioned.

"turn off internet file association wizard"	It is advised to disable the setting.
"turn off printing over http"	To turn off the printing over world wide web protocol http.
"turn off registration if url connection is referring to microsoft.com"	To turn off registration of URL connection if it is referring to Microsoft.com.
"turn off search companion content file updates"	To turn off the companion of search of content file updates.
"turn off the order prints picture task"	To turn off the order of the prints in the task of pictures.
"turn off the publish to web task for files and folders"	Switch off the publishing to the web task of files and folders.
"turn off the windows messenger customer experience improvement program"	Switching off the messenger of windows consumer experience improvement plan.
"turn off windows error reporting"	Windows error reporting switching off.
"always use classic logon"	Usage of classic logon is promoted.

"Do not process the run once list"	Run once list should not be promised.
"require a password when computer wakes on battery"	Password requirement whenever computer wakes up on battery.
"require a password when computer wakes plugged in"	Password requirement whenever a computer plugged in is woken up.
"offer remote assistance"	To offer remote assistance is prohibited.
"solicited remote assistance"	Solicited remote assistance is also prohibited.
"turn on session logging"	Turning on of the session logging.
"restrictions for unauthenticated rpc clients"	Offer unauthenticated restriction for rpc clients.
"rpc endpoint mapper client authentication"	Mapping client authentication for rpc endpoint.
"microsoft support diagnostic tool turn on msdt interactive communication with support provider"	To switch on the support diagnostic tool of Microsoft on msdt interactive communication with the respective support provider.
"allow user to access online	To allow a user to troubleshoot to accessing online content.

troubleshooting content on Microsoft servers from the troubleshooting control panels"	
"Enable disable perftrack"	Enabling and disabling processing of the performance events.
"Configure windows ntp client"	Setting the parameters for monitoring the NTP clients for windows.
"Turn off program inventory"	Managing the state of program inventory collector in the operating system.
"Default behavior for autorun"	Setting the autorun in operating system.
"Turn off autoplay"	Autoplay should be turned off.
"Turn off auto play for non-volume devices"	Determining whether autoplay is off for non-volume of non-indexed devices.
"enumerate administrator accounts on elevation"	Administrative account should be enumerated while elevating.
"do not allow digital locker to run"	Digital locker should be run.
"override the more gadgets link"	More gadgets link should be overridden.

"restrict unpacking installation of gadgets that are not digitally signed"	Enabling this property is recommended since it allows system not to unpack or install not signed gadgets.
"turn off user installed desktop gadgets"	Disabling the gadgets installed by the user.
"maximum application log size"	There should be a max size defined.
"maximum security log size"	There should be a maximum size defined.
"maximum setup log size"	There should be a maximum size defined.
"maximum system log size"	There should be a maximum system log size.
"turn off downloading of game information"	To turn off the downloading of different game information.
"turn off game updates"	Switching off game updates.
"prevent the computer from joining a homegroup"	Prohibiting the operating system from joining a homegoup.
"disable remote desktop sharing"	To disable any remote desktop sharing.
"do not allow passwords to be saved"	It should be properly assigned.
"allow users to connect	Determining whether users can connect remotely.

remotely using remote desktop services"	
"always prompt for password upon connection"	It should be enabled.
"set client connection encryption level"	It should be set correctly for encryption at terminal level.
"set time limit for active but idle remote desktop services sessions"	These should be correctly configured.
"set time limit for disconnected sessions"	There should be a set time limit for sessions that are disconnected.
"do not delete temp folders upon exit"	Folders should not be deleted upon exit.
"do not use temporary folders per session"	Temporary folders should not be used.
"turn off downloading of enclosures"	Downloading of the enclosure should be turned off.
"allow indexing of encrypted files"	The encrypted files should be indexed.

"enable indexing uncached exchange folders"	Uncached folder should not be enabled for indexing.
"prevent windows anytime upgrade from running"	Anytime upgrade should be turned off.
"configure microsoft spynet reporting"	Allowing this to communicate will help Microsoft to defend against the malware risk.
"Disable logging"	It should be enabled.
"Disable windows error reporting"	Microsoft will not send any error reports if it is enabled.
"Disable error notifications"	It should be enabled.
"Do not send additional data"	Additional data request would be declined by user of this operating system.
"Turn off data execution prevention for explorer"	Preventing data execution for explorer.
"turn off heap termination on corruption"	Switching off the heap termination on corruption.
"turn off shell protocol protected mode"	Switch of the shell protocol protected mode.
"disable ie security prompt	IE security prompt for windows installer should be disabled.

for windows installer scripts"	
"enable user control over installs"	It bypasses security measures of windows installer it should not be enabled.
"prohibit non administrators from applying vendor signed updates"	It stops users not administrators from installing vendor signature approved updates.
"report when logon server was not available during user logon"	It stops users not administrators from installing vendor signature approved updates.
"turn off the communities features"	Switching off the features of communities.
"windows mail application manual launch permitted"	Permission of windows mail application manual launch.
"prevent windows media drm internet access"	Preventing the digital rights management of windows media from access to the internet.
"do not show first use dialog boxes"	It should be configured properly.
"prevent automatic updates"	It should be configured properly.
"configure automatic	Automatic updates should be configured properly.

updates"	
"reschedule automatic updates scheduled installations"	Automatic updates scheduled installation should be configured properly.
"no auto restart with logged on users for scheduled automatic updates Installations"	The setting must be properly given.
"do not display install updates and shut down option in shut down windows dialog box"	It should be configured properly.
"Games"	It should be allowed to install.
"Internet Information Services"	It should be installed.
"Simple TCPIP Services"	TCPIP services should not be installed.
"Telnet Client"	It should not be installed.
"Telnet Server"	It should not be installed.
"TFTP Client"	It should not be installed.

”Windows Media Center”	It should not be installed.
”Enable screen saver”	Screen saver should be enabled.
”Password protect the screen saver”	Password protection should be enabled.
”Screen saver timeout”	Timeout should be given.
“turn off help ratings”	It should be turned off.
“do not preserve zone information in the attachments”	It should be disabled.
“hide mechanisms to remove zone”	It should be enabled.
Name	Description
“notify antivirus programs when opening attachments”	It should be enabled.
“prevent users from sharing files within their profile”	It should be enabled.
“security patches up to date”	It should be enabled.

References

[1] Information systemAvailable: http://www.businessdictionary.com/definition/information-system.html#ixzz2XA28oFHh

[2] Kevin Gudgion," McAfee Avert Labs Finding W32/Conficker.worm" Avert Labs Services.

[3]Matteo Maria Casalino, Henrik Plate, and Serena Elisa "Configuration Assessment as a Service" Data Privacy Management and Autonomous Spontaneous Security, Springer 7th International Workshop, DPM 2012, and 5th International Workshop, SETOP 2012, Pisa, Italy, September 13-14, 2012. Revised Selected Papers

[4] Arnold Johnson, Kelley Dempsey, Ron Ross, Sarbari Gupta and Dennis Bailey, "Guide for security focused Configuration Management" Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, August 2011.

[5]David Waltermire, Stephen Quinn, Karen Scarfone and Adam Halbardier, "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2" Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, September 2011.

[6] CA Product Validation Information Available: http://nvd.nist.gov/validation_ca.cfm

[7] IBM Product Validation Information Available: http://nvd.nist.gov/validation_ibm.cfm

[8]Adam Halbardier, David Waltermire and Mark Johnson, “Specification for the Asset Reporting Format 1.1” Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, June 2011.

[9] USGCB FAQ(s) Available:http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdc

[10] Whitepaper: Configuration Management Explained, Numara Software

[11] Parker, Donn B. Threats to computer systems. No. UCRL-13574. CALIFORNIA UNIV BERKELEYLAWRENCELIVERMORE LAB, 1973.

[12] Malone, Robert J., and Reuven R. Levary. "Computer Viruses: Legal Aspects."U. Miami Bus. LJ 4 (1993): 125.

[13] D. Moore, C. Shannon, and k claffy.
Code-Red: A case study on the spread and victims of an Internet worm.
In ACM Internet Measurement Workshop, 2002.

[14] Definition of a malware: http://www.studioprovider.com/terms/malware.html

[15] Bayer, Ulrich, et al. "A view on current malware behaviors." USENIX workshop on large-scale exploits and emergent threats (LEET). 2009.

[16]M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis.
A Multifaceted Approach to Understanding the Botnet Phenomenon.
In Internet Measurement Conference (IMC), 2006.

[16] Anubis Information: https://anubis.iseclab.org/?action=about

[17] Radack, Shirley, and Rick Kuhn. "Managing security: The security content automation protocol." IT professional 13.1 (2011): 9-11.

[18] Zhou, Lidong, et al. "A first look at peer-to-peer worms: Threats and defenses."Peer-to-Peer Systems IV. Springer BerlinHeidelberg, 2005. 24-35.

[19] Weaver, Nicholas, et al. "A taxonomy of computer worms." Proceedings of the 2003 ACM workshop on Rapid malcode. ACM, 2003.

[20] Serazzi, Giuseppe, and Stefano Zanero. "Computer virus propagation models."Performance Tools and Applications to Networked Systems. Springer BerlinHeidelberg, 2004. 26-50.

[21] Moskovitch, Robert, Yuval Elovici, and Lior Rokach. "Detection of unknown computer worms based on behavioral classification of the host." Computational Statistics & Data Analysis 52.9 (2008): 4544-4566.

[22] Thimbleby, Harold, Stuart Anderson, and Paul Cairns. "A framework for modelling trojans and computer virus infection." The Computer Journal 41.7 (1998): 444-458.

[23] Wang, Chenxi, John C. Knight, and Matthew C. Elder. "On computer viral infection and the effect of immunization." Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference. IEEE, 2000.

[24] David Waltermire, Stephen Quinn, Karen Scarfone and Adam Halbardier “The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2”

[25] Gary Locke, Secretary Patrick D. Gallagher “NIST Special Publication 800-128”

[26] Montesino, Raydel, and Stefan Fenz. "Information security automation: how far can we go?." Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. IEEE, 2011.

[27] Montesino, Raydel, and Stefan Fenz. "Automation possibilities in information security management." Intelligence and Security Informatics Conference (EISIC), 2011 European. IEEE, 2011.

[28] Molavi, Mehran, and Amir Makali. "Security Management Information Systems According to Standards."

[29] Nainar, M. Asan, and Abdul Rasheed. "Dynamic Security Technique for Content Management Repository System." International Journal 2.1 (2014).

[30] Alsaleh, Mohammed Noraden, and Ehab Al-Shaer. "Scap based configuration analytics for comprehensive compliance checking." Configuration Analytics and Automation (SAFECONFIG), 2011 4th Symposium on. IEEE, 2011.

[31] Saroiu, Stefan, Steven D. Gribble, and Henry M. Levy. "Measurement and Analysis of Spyware in a University Environment." NSDI. 2004.

[32] Saroiu, Stefan, Steven D. Gribble, and Henry M. Levy. "Measurement and Analysis of Spyware in a University Environment." NSDI. 2004.

[33] Ganapathi, Archana, et al. "Why pcs are fragile and what we can do about it: A study of windows registry problems." Dependable Systems and Networks, 2004 International Conference on. IEEE, 2004.

[34] Yi-Min Wang, Chad Verbowski, John Dunagan, Yu Chen, Helen J. Wang, Chun Yuan, and Zheng Zhang, “STRIDER: A Black-box, State-based Approach to Change and Configuration Management and Support,” Proc. Usenix Large Installation Systems Administration (LISA) Conference, pp. 159-171, October 2003.

[35] Apap, Frank, et al. "Detecting malicious software by monitoring anomalous windows registry accesses." Recent Advances in Intrusion Detection. Springer BerlinHeidelberg, 2002.

[36] Kim, Youngsoo. "Windows registry and hiding suspects' secret in registry."Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, 2008.

[37] Research Methodology Information http://www.thefreedictionary.com/Research+methodology

[38] SCAP validated products http://scap.nist.gov/validation/index.html

[39] Shannon, Claude Elwood. Claude E. Shannon: Collected Papers. Eds. N. J. A. Sloane, and Aaron D. Wyner. John Wiley & Sons, 1993.s

[40] Machine, Universal Turing. "The undecidable: Basic papers on undecidable propositions unsolvable problems and computable functions." (1956).

[41] Security and Network Effects: Centralized and Decentralized Networks: http://www.sigecom.org/exchanges/volume_10/3/VOROBEYCHIK.pdf

[42] Runeson, Per, and Martin Höst. "Guidelines for conducting and reporting case study research in software engineering." Empirical software engineering 14.2 (2009): 131-164.

[43] Easterbrook, Steve, et al. "Selecting empirical methods for software engineering research." Guide to advanced empirical software engineering. Springer London, 2008. 285-311.

[44] Järvinen, Pertti. "Action research is similar to design science." Quality & Quantity 41.1 (2007): 37-54.

[45] Development team of MCS for inhouse development of application and management of assets: http://www.nust.edu.pk/INSTITUTIONS/Colleges/MCS/Pages/DevelopmentTeam.asp

[46] Local security policy: https://technet.microsoft.com/en-us/library/dd277395.aspx

[47] Group policy: https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx