bradscholars

A Quantitative Security Assessment of Modern Cyber Attacks. A Framework for Quantifying Enterprise Security Risk Level Through System's Vulnerability Analysis by Detecting Known and Unknown Threats

Item Type	Thesis
Authors	Munir, Rashid
Rights	 The University of Bradford theses are licenced under a Creative Commons Licence.
Download date	2025-04-26 20:15:25
Link to Item	http://hdl.handle.net/10454/14251

UNIVERSITY of BRADFORD Library

University of Bradford eThesis

This thesis is hosted in Bradford Scholars – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team

© University of Bradford. This work is licenced for reuse under a Creative Commons Licence.

A QUANTITATIVE SECURITY ASSESSMENT OF MODERN CYBER ATTACKS

R. MUNIR

Ph.D

2014

A Quantitative Security Assessment of Modern Cyber Attacks

A Framework for Quantifying Enterprise Security Risk Level Through System's Vulnerability Analysis by Detecting Known and Unknown Threats

Rashid MUNIR

Submitted for the degree of
Doctor of Philosophy

Faculty of Engineering and Informatics

University of Bradford

2014

ABSTRACT

Rashid Munir

A Quantitative Security Assessment of Modern Cyber Attacks

A Framework for Quantifying Enterprise Security Risk Level Through System's Vulnerability Analysis by Detecting Known and Unknown Threats

Keywords: Enterprise Network Security; Vulnerability Analysis; Security Assessment; Common Vulnerability Scoring System (CVSS)

Cisco 2014 Annual Security Report clearly outlines the evolution of the threat landscape and the increase of the number of attacks. The UK government in 2012 recognised the cyber threat as Tier-1 threat since about 50 government departments have been either subjected to an attack or a direct threat from an attack. The cyberspace has become the platform of choice for businesses, schools, universities, colleges, hospitals and other sectors for business activities. One of the major problems identified by the Department of Homeland Security is the lack of clear security metrics. The recent cyber security breach of the US retail giant TARGET is a typical example that demonstrates the weaknesses of qualitative security, also considered by some security experts as fuzzy security. High, medium or low as measures of security levels do not give a quantitative representation of the network security level of a company. In this thesis, a method is developed to quantify the security risk level of known and unknown attacks in an enterprise network in an effort to solve this problem. The identified vulnerabilities in a

case study of a UK based company are classified according to their severity risk levels using common vulnerability scoring system (CVSS) and open web application security project (OWASP). Probability theory is applied against known attacks to create the security metrics and, detection and prevention method is suggested for company network against unknown attacks. Our security metrics are clear and repeatable that can be verified scientifically.

Dedicated to my beloved parents, wife and sisters

ACKNOWLEDGEMENTS

All praise is Due to Allah Subhanahu Wa Ta'ala for His Glorious Ability and Great Power as He has given me the power, patience, ability and knowledge to complete this doctoral thesis. All respects to Holy Prophet Hazrat Muhammad (P.B.U.H) who is the last messenger, who has given us a complete code of life.

I would like to thank my supervisor Prof. Irfan Awan for his guidance, encouragement and continuous support through the course of this work. He stimulated my interest in the field of network security and also improved my ability to teach and to manage a group of people. I would also like to acknowledge my second supervisor Dr. Jules Ferdinand Pagna Disso for his useful comments and suggestions during this work. Special thanks to Dr. Muhammad Rafiq Mufti for his help while designing mathematical models and proofreading my research work.

My gratitude for financial support goes to the University of Bradford.

I am deeply indebted to my Nani Amman, Grandfather, Aziz Dutt, Asif Dutt, parents, sisters, brothers Shehzad Munir and Arshad Munir, my wife and two little daughters Aiza and Hibah for their understanding, endless patience and encouragement when it was required.

I would like to express my sincere thanks to Tariq Maqsood, Asmi Darr, Nasir Khan, Dr. Faeiz Alserhani, Zeenat, Farhat, Shafeen, Dr. Adeeb Alhomoud and Anitta namanitta for their support and encouragement during the tough time at Bradford.

I am also grateful to all my friends especially Iftikhar Siddique, Khurshed, Shahzad Nazir and Qaiser Naeem for their well wishes during my research work.

May Allah Subhanahu Wa Ta'ala bless all of them.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CIFS	Common Internet File System
CNA	Computer Network Attack
COPS	Computer Oracle and Password Systems
CVSS	Common Vulnerability Scoring System
FIRST	Forum of Incident Response Team
ICT	Information Communication Technology
IE	Internet Explorer
IT	Information Technology
MS-RDP	Microsoft Remote Display Protocol
NetSPA	Network Security Planning Architecture
NIAC	National Infrastructure Advisory Council
NIDS	Network Intrusion Detection System
OISF	Open Information Security Foundation
SCADA	Supervisory Control and Data Acquisition
TVA	Topological Vulnerability Analysis
US-CERT	United State - Computer Emergency Response Team
VA	Vulnerability Assessment
VST	Vulnerability Scanning Tool

Chapter 1.

INTRODUCTION

1.1 Introduction

The Internet is evolving at a remarkable rate in all areas of society. Nowadays, it is recognized as a de facto standard for data communication especially for large organizations such as government agencies, laboratories and universities having a large number of potential users [1]. The prompt increase in Internet traffic and emerging complexities in computer network activities has led to growing network attacks through the Internet, which has put a great impact on the security requirements (availability, confidentiality and integrity) of critical data information. These attacks cause disruption to business processes leading to increase the risk associated to the security of the information technology (IT) systems [2], [3]. It is however, important to ensure that despite these attacks, computer systems continue to operate and deliver the services they are intended for.

Firewalls, antivirus and, network intrusion detection and prevention (NIDP) systems are some examples of the security countermeasures which are deployed by most of the organizations to prevent their assets against malicious intrusion [4]. In small organizations, security management uses conventional scanning tools such as firewalls and antivirus programs to detect and prevent networks from malicious attacks, but these tools generate too many false positives and also have very limited attack detecting rate. Whereas at enterprise network, NIDP systems are the security

countermeasures used to detect and prevent attacks occurring on the network. Despite of the availability of current security countermeasures, still, it is difficult to determine the security risk level of a network.

According to [5], determination of security level depends upon factors such as threats, policy updates, emergence of new vulnerability and network traffic. Among these factors, vulnerability plays a key role in exploiting a network since it gives invitation to intruders to attack the network. The bigger the network, the higher will be the number of vulnerabilities, therefore leading to higher level of security risk [6], [7].

Quantification of network security risk level is a tedious and lengthy process. However, it is less challenging to assess the security risk level of a small organization with limited resources as compared to a large organization having complex infrastructure. Hence, at an enterprise network level, there is a need to design automated tools that can evaluate the impact of all vulnerabilities present in it. For this purpose, security management uses various kinds of vulnerability scanning tools (VST) [4] to assess vulnerabilities in a network. The results produced by these VST can be helpful to any network administrator to determine the qualitative security risk level. These results are expressed in terms of fuzzy values such as low, medium and high, which do not describe the overall associated network security risk level quantitatively.

Nowadays, security community's major concern is to solve open research questions such as hardening a network with less effort, interpreting the relationships among the resources and determining the techniques used by

attackers to achieve their targets. Less efforts have been made towards quantitatively measuring the overall security risk level of enterprise networks [8], [9], [10].

Network attack graph is one of the most prominent solutions used in network security because it gives details of all the possible attack paths due to vulnerability. This evaluation system helps IT management to increase the performance and secure their network by remediating the high prone vulnerability with low prone vulnerability. It, however, does not provide the overall quantitative security risk level of an enterprise network [11]. It was suggested by [12] that to determine the security risk level of an organization, metrics are considered as a helpful approach. Network security is only manageable if it can be measured. Therefore, the introduction of quantitative metrics to measure overall network security risk level can assist the organizations prioritising threats and vulnerabilities.

1.2 Why creating security metrics is so tough?

While creating a metric, there are two questions that need to be answered: the “What”, and the “How”. The “What” is answered by the object that needs to be quantified. The “How” is answered by the repeatability, clarity and authority of the metric created for. The main objective is to make clear statement of what is to be measured as well as usefulness of the metric. There is a need to look at the methods deployed to achieve repeatability of that metric. For example, looking at some classic metrics in other disciplines such as data centre service level agreement, the metrics used are mean time

to failure (MTTF), mean time to repair (MTTR), availability and response time. The classic metrics used by organizations are as follow:

- Mean time between failures (MTBF) is the frequency of failure;
- MTTR is the duration of failures once it occurs;
- Availability is just the probability that the user needs to access the service when it is required and
- Response time deals with the quality of the service.

Organizations use the above-mentioned metrics to measure, monitor and evaluate their systems. Particularly, these metrics are employed to define the desired service levels in most agreements. In an enterprise network security, the questions that are always raised by the organizations are:

- Are we secure?
- Are we spending too much in terms of time or money?

Although, these are good questions in principle but in general, it is difficult to answer them efficiently. Defining the metrics to answer some of these questions requires a detailed breakdown of the question into number of questions that target specific smaller areas to contribute the bigger picture. Presently, security tools answer these questions in terms of high, medium and low. These are qualitative metrics which do not convey the effectiveness of the network security management system. Quantitative metrics can provide a better picture of the security risk level in the enterprise network. In order to create quantitative metrics for the network security risk level of an enterprise network, there is a need to identify the 4-tuples associated to the

risk; 1) the vulnerability, 2) the threat due the vulnerability, 3) the impact of the threat and,4) the value of affected assets in case if threat is successful.

1.3 Motivation

As, the number of attacks are increasing, it is becoming increasingly apparent that many companies do not apply appropriate risk management techniques [13], [14], [15]. It is suggested by [16] that companies can reduce their risk posture if they apply basic risk management techniques by about 80%. Statistics shows that the challenges in protecting companies are fast growing. It is not possible any more to ensure a good security level by just relying on blocking the attacks as they appear. A number of security initiative such as intrusion detection system (IDS), intrusion prevention system (IPS) and antiviruses are mostly reacting to security events. In order to create a successful signature, an event/attack needs to be happened. However, a report by [13] shows that attacks are being used new ways to attack companies.

Many businesses and even country stability have been affected by successful cyber-attacks. In order to reduce the impact of these attacks, this work is looking at how organizations can have a better understanding of their security level. Qualitative risk analysis has been beneficial but it does not provide a quick and easy way to understand the security level of a company. This thesis is developed with the ambition to support the security communities in providing a new method to quickly and easily understand security risk level. As a result of this new metric system, the companies can quickly react to challenges.

1.4 Aims and Objectives

The basic aim of this research is to develop a method that quantitatively assess the security status or risk level of IT networks in terms of attacks. The main objectives of this research are:

- Evaluation of an existing UK organization for the purpose of classifying and identifying the vulnerabilities contained in a real network.
- Developing a security metric based on measurements in the form of vulnerabilities gathered from the network.
- Applicability of probabilistic theory to determine the overall security risk level of each department and entire organization's network in terms of absolute value.
- Analysis of various attacks to define the invisible attack.
- Introducing a method of assessing the security risk level of IT networks in terms of invisible attacks, and providing a solution to detect and prevent from these invisible attacks by incorporating enterprise network security countermeasure.
- Performance comparison of enterprise security countermeasures Snort with Suricata for the purpose of selecting the best NIDP system in terms of packet handling capability for creating NIDS security metrics based on different traffic speeds.

1.5 Research Contributions

The main contributions of this research are:

- To develop a security metrics based on the measurements in the form of vulnerabilities collected from an existing UK organizational network.
- To analyse various attacks to define the invisible attack and introduce a new method of assessing the security risk level of IT networks in terms of invisible attacks.
- Performance comparison of enterprise security countermeasures Snort with Suricata for the purpose of selecting the best NIDP system in terms of packet handling capability for creating NIDS security metrics based on different traffic speeds.

1.6 Organization of the Thesis

Following this introduction, Chapter 2 gives some overview of basic security parameters such as risk assessment, metrics etc. followed by a detailed background information to understand the entire thesis.

A novel security metric is introduced in Chapter 3 to evaluate the security risk level of any enterprise IT network using probability theory by incorporating vulnerability scanning tool (VST). Probabilistic approach is then applied to calculate the overall security risk level of sub-networks and entire network. These metrics can be valuable for any network administrator acquiring an absolute risk assessment of a network.

In Chapter 4, a new method is proposed to quantitatively evaluate the security risk level of invisible attacks. This chapter provides the classification of all invisible attacks according to their characteristics against IT, business network and critical infrastructure. A way to detect and prevent organization from invisible attacks is suggested and then the security risk level is estimated.

Chapter 5 deals with initial research phase to carry out a performance evaluation of NIDP systems as a background to our preliminary testing. Extensive testing scenarios are implemented on a highly sophisticated test-bench using various platforms and configurations. A detailed performance of Snort as a de facto IDS standard versus Suricata is investigated under different traffic conditions. The tests are conducted on host and virtual systems configurations to explore the system response in different deployments. Packet drops as an identified limitation of software-based IDS in high-speed environments is discussed in this chapter. A security metric is also developed based on the results achieved from the experiments.

In Chapter 6, a brief review of the results of the previous chapters along with some general comments is given and proposed future work is also presented.

Chapter 2.

BACKGROUND AND RELATED WORK

Network security is the most vital component in information security as it is responsible for securing all information passed through networked computers. In order to understand how to secure a network, the concepts and literature related to network security need to be reviewed. The methods that are the building blocks of designing the network security risk metrics and the different standards as used in network security are also discussed therein.

2.1 Network Security

This section describes security properties, vulnerabilities and attacks.

2.1.1 Security Properties

In information technology (IT), security is the logic of prevention malware to enter into a system or a network. It is also called a degree of protection against intrusion in hostile environment and is defined as "*Measures adopted to prevent an unauthorised use, misuse, modification, or denial of use of knowledge, facts, data or capabilities*" [17]. According to [18], security is particularly a combination of three main properties: confidentiality, integrity and availability of information. The brief description of each property is given as follows:

- Confidentiality

Confidentially is also known as secrecy or privacy. It refers to the assurance that the computer related assets are only accessed by the authorized parties [19], [20], [21].

- Integrity

It is the assurance that information can only be accessed or modified by the authorized users. It ensures that network messages remain complete, correct and authentic, and are not modified by unauthorized parties [20], [21].

- Availability

This property ensures that only authenticated users having specific authorization can access system and work with information, assets and resources when required [22], [23].

2.1.2 Vulnerability

Vulnerability is the manifestation of the inherent state of the system which is exploited by intruder to damage/harm the system or network. It can also be called a flaw, bug, weakness or an exposure of an application. In IT security, it performs a special role in opening the ways for attackers to endanger computer system's security [24], [25]. An Attacker can take advantage of a vulnerability holes to disrupt a network to achieve the target. According to Computer Emergency Response Team (CERT), the numbers of vulnerabilities are increasing due to increase in computer usage and its resources [26].

2.1.3 Attacks

With the advancement in technology and the increasing dependencies of our societies on usage of network information systems, the risk of attacks on networks especially at enterprise level has been tremendously increased [27]. In computer terminology, attack or threat can be defined as an attempt to compromise security properties of a system or communication network [28]. According to [29], an attack is a specific technique designed to exploit a vulnerability contained in the configuration, implementation or management of an entity to achieve the desired target. Three conditions must be met for any attack to be carried out against an enterprise network;

- The network under attack should have vulnerabilities that can be exploited.
- The resources available to the threat agent must be sufficient to carry out the attack in mind.
- The attacker must be driven by a motive whether it is recreational, profit oriented or vengeance.

When these conditions are satisfied, an attack is said to be eminent. Analysis of the vulnerabilities in the enterprise network is the first step in ensuring that the network is guarded against attacks [30]. Depending on their nature, attacks can be classified into two main categories: physical attacks and cyber attacks [31].

2.1.3.1 Physical Attacks

Physical attacks also called insider attacks are generated from inside the organization by legitimate users based on level of authority granted to them [32], [33].These attacks intentionally violate the organization security policies. Figure 2.1 shows some of the examples of physical attacks. As, most enterprise networks have policies to prevent against exportation of information from the company by blocking the use of unauthorized external storage drives. DeviceLock, Sanctuary Device Control, USB blocker to mention but a few are some of the tools and applications used at the enterprise level to monitor the workstations and enforce the policies.

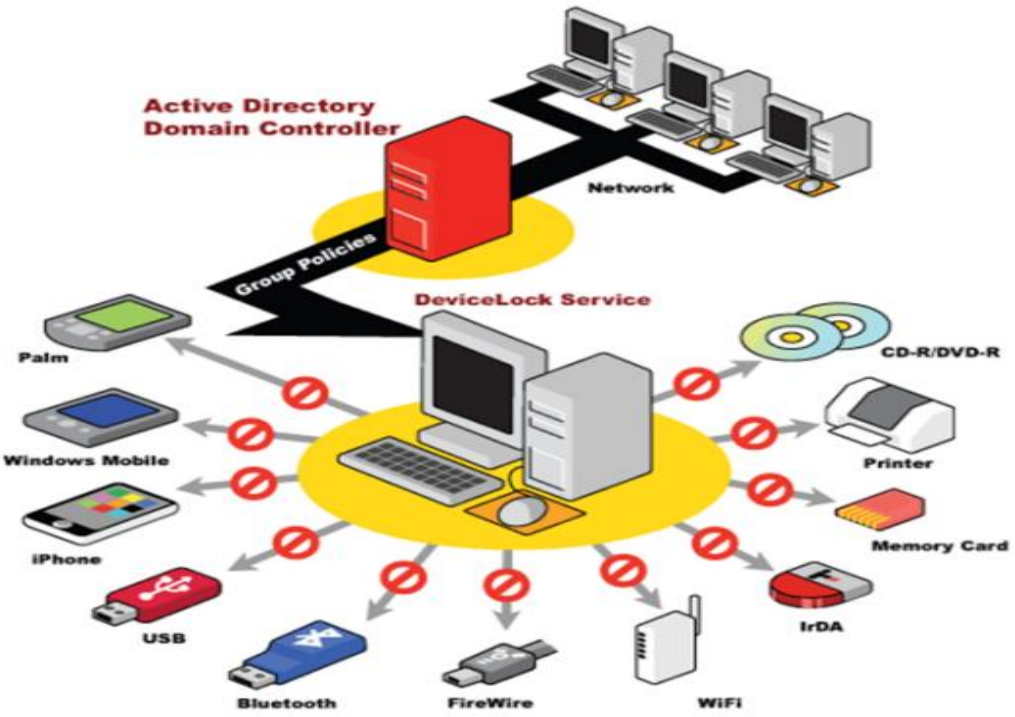

Figure 2.1: Organizations' insider attacks [34].

There are also ways of manipulating Windows Group Policy Objects (GPO) to restrict USB access but this has been difficult to achieve in practice. If an

enterprise does not enforce these kinds of policies and external drives are allowed unto the network, a disgruntled employee is able to bring in an infected drive. Once this drive is installed/ plugged into the workstation, the network is easily compromised as it is attacked from inside the organization from a legitimate source.

2.1.3.2 Cyber Attacks

These attacks are also called outsider attacks or computer network attacks (CNAs). It is a deliberate attempt employed by individual or group of people to:

- Damage computer networks;
- Gain unauthorized access to computer system or a network and
- Disrupt business infrastructure processes and equipment operations by hacking into a vulnerable system.

➢ Cyber Attacks Characteristics

Cybercriminals opportunistically scan the Internet against information communication technology (ICT) systems having some pre-existing vulnerabilities such as lack of antivirus, security countermeasures, weaknesses in installed programs or faulty system. The system containing vulnerabilities is considered most susceptible of cyber attacks. Once the system exploited via malicious code, it can be easily controlled by an attacker [35]. Figure 2.2 depicts some of the possible cyber attacks on enterprise network.

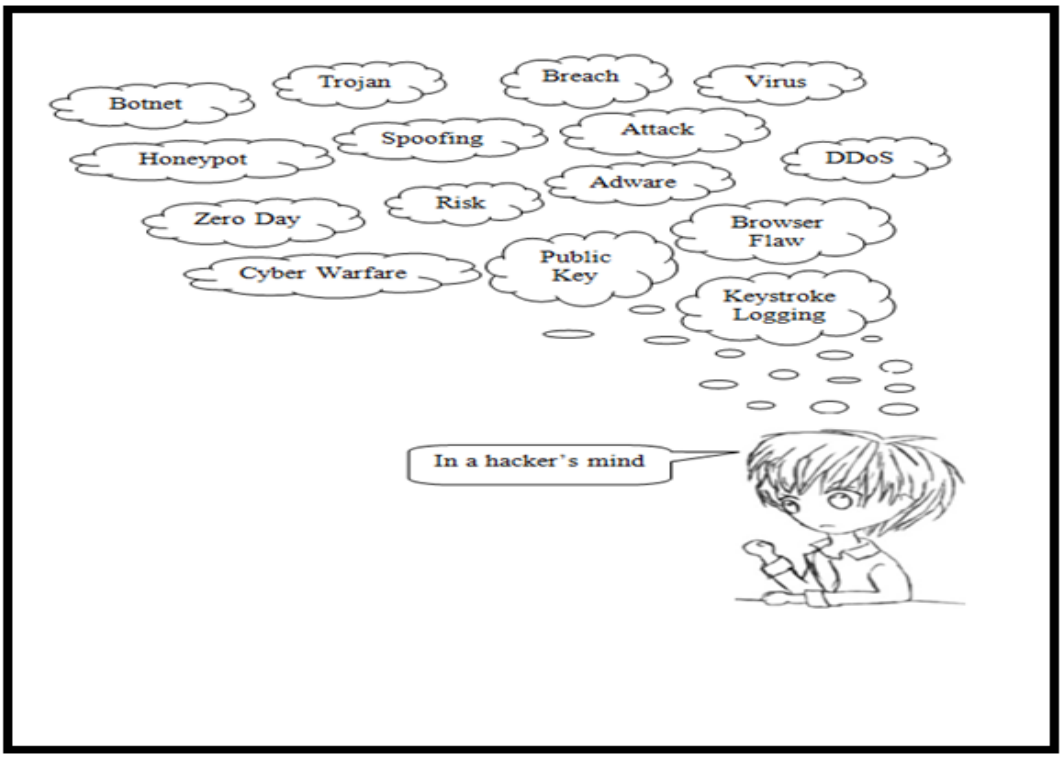

Figure 2.2: Cyber-psychopathic.

2.2 Risk

In IT, risk can be defined as a potential that a chosen action or activity lead to loss. It determines the possible impact of attack on a particular system or network through vulnerability. Information security risk assessment identifies, measures and prioritizes the risks based on attack impact, likelihood and affected IT assets. According to [36], risk is the product of the likelihood of an event occurred and its impact on information technology assets, i.e.

$$Risk = Attack\ likelihood * Impact$$

Moreover, the impact of an event on an information asset is further equal to the product of asset vulnerability and asset value to its stakeholders. Now, IT risk can be equal to:

Risk=Attack likelihood Asset value* Vulnerability*

Thus, in the light of the risk equation, the threat (Attack likelihood), asset value and vulnerability are the most critical parameters in measuring the overall security risk that should be taken into account. Asset value is the easiest to measure among the three parameters [37]. In IT security, the basic components of security risks are vulnerability, capability and threat, where the term capability refers to the adversary ability and capacity to access the target.

2.3 Metrics

In IT security, metrics are used to quantify the results achieved through a set of measurements. The enterprise level organizations use various metrics to meet their desired targets. For example, security metrics are used to determine how much organization is secure enough. Business metrics describe business progress in a measurable form. Project metrics are used for the projects to determine whether the goal is achieving or not.

Metrics provide companies a way to prioritize their threats and vulnerabilities, and calculate the risks posed on information assets depending upon quantitative or qualitative measurement [38]. Qualitative metrics define the assessment process leading to non-numerical value and are hard to analyse. On the other hand, quantitative metrics are easy to understand. These are normally in numerical form and are often used for ranking purpose.

Metrics and measurements are two different types of entities. Metrics are derived from comparison of two or more sets of mathematically relevant and

quantifiable attributes taken over a period of time, e.g. the number of attacks detected by intrusion detection systems (IDSs). Measurements are numeric values generated through counting and are assigned to a specific attribute based upon pre-defined criteria. These are usually called objective raw data and specify the number of dimension, size and quantity of a particular attribute of a process or product, e.g. the number of IDSs used to prevent network against malicious activity.

2.3.1 Categories of Security Metrics

Security metrics are classified into three categories, as follows:

- Organizational Metrics

These metrics are related to industry operators or users of supervisory control and data acquisition (SCADA) control systems, and play an important role in making decisions such as which assets are critical to attack? Are the protections in place sufficient to protect the information?

- Operational metrics

These metrics describe security posture, risk management, support measures, threat environment, incident response and vulnerability management practices of an organization. These should refer to the factors or attributes being affected by risk related situations.

- Technical metrics

These metrics describe and compare technical objects like algorithms specifications and architectures, alternative designs products, etc. These are generally associated with technical standards, supports of IT products,

technologies, architectures and level of risk to operate a system in a given configuration environment.

2.3.2 Security Metrics Significance

Metrics are helpful tools for security analysts in identifying the level of risk in the organizations. These tools can be used to distinguish the effectiveness of different components of security programs and also increase the level of security awareness within the organization [37], [39]. Metrics make easier for analyst to answer hard questions raised from higher authorities such as:

- How do we compare to others in this regard?
- Are we secure enough?
- Are we more secure than yesterday?
- How much the current network is secure?
- How vulnerable is this network to specific attack mechanism?

2.4 Intrusion Detection Systems

The prevalent use of sophisticated technologies like web services, remote access and distributed database in networks communities has raised new issues in terms of network security. To protect these networks from malicious attacks, the most sophisticated tools are required to provide accurate and reliable protection against malware. An intrusion is defined as a malicious internally or externally operational fault or the result of partially or completely successful attack [40]. To detect and prevent intrusion at an enterprise level, the IDSs are utilized. These are a combination of hardware and software that

generate alert when any intrusion occurs [41]. The idea of IDS was first introduced in 1980 by James Anderson when he distinguished between the characteristics of anomalous and normal behaviour in the anomaly detection approach [42]. The IDSs have been developing in the response to unwanted malicious traffic that may potentially compromise the functionality of the network [43]. One of the key features of any IDS is to analyse the activities running on the system and to monitor the data provided by the users. The IDS generally comprises several components operating in conjunction to offer protection against malicious activities. Main IDS components are as follows:

Sensors: The IDS sensor sits upon the network and logs the traffic after sniffing it in a promiscuous mode and generates an alert on the console.

Console: The IDS console provides user interface, where a network administrator may take notice of any current attack alerts.

2.4.1 Types of IDS

Based on the location in a network, IDS are broadly classified into two main categories: Host based IDS and Network based IDS.

2.4.1.1 Host based IDS

Host based IDS (HIDS) is installed locally on a host computer and is capable to analyse that traffic which is coming to and originating from the particular computer. In case of attacks by other than the particular computer on network, HIDS cannot be able to detect it. HIDS has ability to monitor system activities such as files access system of a host, host network traffic, users'

logon activities, running processes, computer integrity and windows registry, etc. OSSEC is an example of HIDS, which is an open source platform dependent tool supporting OpenBSD, Macintosh, Window and Solaris operating systems. Some of the advantages of HIDS are as follows:

- They have the ability to verify whether the attack was successful or not.
- They can identify those attacks that originate from inside the host.
- Since, HIDS can analyse the decrypted traffic to estimate attack signature thus leading to monitor encrypted traffic as well.
- These are cost effective for a small network of few computers.

However, HIDS has some drawbacks.

- They can be compromised immediately as the host server is compromised by an attack.
- They consume more computing power from the host where it is installed.
- In case of denial of service attacks, their performance is not effective.

2.4.1.2 Network Based IDS

Network intrusion detection and prevention (NIDP) systems are set up in a network to monitor traffic for any suspicious activity in order to prevent the network from being compromised. These systems run as an independent platform treating network traffic as a supply of data. A NIDP system uses predesigned policies to detect any unauthorised activity on the network. It

performs a deep search of the monitored in-coming and out-going traffic to detect malicious packets in a network. Once it detects a malicious packet, it informs the system administrator through an alert or blocks that malicious packet to avoid network compromise. A NIDP system contains a group of sensors that are positioned on tactical ends to capture the traffic on a network. SNORT is an example of NIDP systems. These systems are always used in addition to other security countermeasure tools like firewalls and anti-virus systems. The NIDP systems in addition to network monitoring functions can also perform other duties which include:

- Maintains data and file integrity by scanning the system files for any unauthorized activity.
- Detects any changes in the server core components.
- Matches known remote hacking attempts or network compromise patterns by scanning the server log files.
- Scans local firewalls or network servers for any potential exploits.

One of the shortfalls of the NIDP systems is that it depends upon the policy design to protect the network. So misconfiguration can lead to exposure of the network or false positives on the network. False positives are created when legitimate traffic is treated as suspicious traffic. NIDP system products have always built in policies which can be rewritten to customize to the specific organization. The systems also allow new policies to be written into the configuration file. The policies defining the traffic monitoring rules are what to be used to generate alerts in case of any suspicious activity. These

rules fall into two categories: 1) the default rules provided by the product vendor are classified according to CVSS standard, and 2) the customised rules written by the organization's network management team can be classified using the preferred network security standard.

The rules created in NIDP system help the network management to assess the security risk level of their network based on the priority attached to the attack impact associated with the rule.

2.5 Vulnerability Scanning Tools

Vulnerability assessment (VA) tools also called security scanning tools provides help in scanning firewalls, network and software applications. These tools run on the periodic basis and are generally used to generate the vulnerability reports of technical and management issues in the form of texts, charts or graphs, which are useful for companies' network administrators to make their network secure. Following is a comparison of some of the popular VA tools.

Table 2.1: Comparison of Vulnerability Scanning Tools.

Features	**Tools**				
	Nessus	**Nexpose**	**SAINT**	**Nipper**	**Retina**
Commercial	✓	✓	✓	✓	✓
GUI	✓	✓	✓	✓	✓
Home feed version scans up to	16	32	16	32	256

IP addresses					
Cost per year	£600	£15400 per user	£5200	£26 per device	£750
Supported platforms	Kali Linux, Fedora, Mac OS, Red Hat, Linux, Win XP & above, Server 2003 & above	Kali Linux, VM ware ESXi, Red Hat, Win 7 &above, Server 2008 &above	Linux, Mac OS, OpenBSD, FreeBSD	Fedora, Mac OS, Centos, Linux, OpenSuSE, Ubuntu	Windows XP and above, Windows Server 2003 &above
Supported Browsers	Safari, Firefox, Google Chrome, Opera, IE 10 & above	IE 9 &above, Mozilla Firefox, Google Chrome	IE 9, Firefox, Safari	-	-
System hardware requirements	3-4GB RAM	2 GHz Processor, 100 Mbps NIC 10+GB disk space	2 GB RAM	1 GB RAM &250 MB disk space	1.4 GHz Processor, 512 MB RAM &1GB disk space

Now the characteristics of the VA tools are discussed as follows.

2.5.1 Nessus

It is one of the popular VA tools, which was initially free and open source till 2008 [44]. It is helpful in configuring, patching and auditing the networks and provides a platform for compliance monitoring, vulnerability management, IT risk management, attack detection and mitigation. It is regularly updated by more than 46,000 plug-ins [44]. Some of its features are:

- It scans those vulnerabilities that can be exploited remotely to access network data or systems.
- It scans any misconfiguration in the network, for example, missing patches.
- It scans weak passwords used in the network, where it sometimes launches hydra to perform a dictionary attack.
- It scans the presence of invalid packets using the TCP/IP which can be used for denial of service attacks.
- It helps in auditing the payment card industry data security standards.

2.5.2 Nexpose

It is a universal vulnerability management tool providing reliable and prompt decisions to assess the security risk level of networks [45]. Its key functions are to detect, assess and mitigate the security risk level exposed by vulnerabilities, misconfigurations and policy violations, and to analyze malware in any IT environment having different operating systems, web applications and databases. Because of its features, it is highly efficient than

other VA tools. It is a stand-alone software providing user interaction through web browser [45]. It works with Metasploit (attack generating tool) to exploit vulnerabilities and calculates their weightage through CVSS, and then validates the security risk.

2.5.3 SAINT

The conventional tools describe fuzzy security risk level of a network by incorporating vulnerability severity level (VSL) prioritization such as high, medium and low [46]. The SAINT Corporation takes this prioritization to the next level by providing the ability to sort, filter, and prioritize threats by mapping industry-recognized identifiers. Its main functions include:

- Identifying exploitable vulnerabilities on the networks and its resources.
- Detecting and fixing any point of weakness before exploitation.
- Anticipating and preventing common system vulnerabilities.
- Auditing the systems and configurations for compliance with regulatory standards.
- Scanning the content of the network nodes for data that is not authorized to be stored there.
- Generating the vulnerability assessment repots in the specified formats.

2.5.4 Retina

It is a commercial VA tool written by well-known security research team called eEye [46]. It is used to efficiently assess the security risk level by discovering, fixing and prioritizing vulnerabilities of enterprise network. It provides fast, flexible deployment to increase remote and local security across all IT assets. It uses a regularly updated vulnerability database.

2.5.5 Network Infrastructure Parser (Nipper)

This tool is used to assess the security risk level of network devices such as firewalls, routers, and switches [46]. Before the release of Titania software, Nipper was used as a free open source tool for analysing device configuration file. Its security audit [46] report contains the detail regarding software versions, authentication passwords, authentication services, VPN configuration, Web services, time synchronization, logon messages, name resolution services, firewall rules, intrusion detection/prevention, routing protocols, cryptographic settings, logging and printing services etc.

2.5.6 Secunia Personal Software Inspector

It is also a free scanning tool designed to detect vulnerable and outdated programs, and plug-ins, which provide invitation to attack the system [46]. It is normally run on a stand-alone machine but at an enterprise level, Secunia corporate software inspector tool is employed to scan more than one computer in a network.

2.5.7 Open Vulnerability Assessment System

Open Vulnerability Assessment System (OpenVAS) is an open source VA tool [46]. It is easy to use having less plug-ins than Nessus. Most of the OpenVAS components are licensed with GNU. This tool is updated on daily basis because of supporting high standard organizations.

The VST are helpful in network security assessment, and network administrators use them to determine the list of existing vulnerabilities on a system or network [46]. Although the achieved information is useful, but not enough to measure the network security risk level. If the vulnerabilities listed as many, there is need for other methodologies to be employed to group and quantify these vulnerabilities. The security metrics proposed in this work is able to take this list of vulnerabilities and provide a single value representing the absolute overall security risk assessment level of the network.

2.6 Related Work

Measuring security metrics have always been a big challenge due to various reasons. For instance, the security posture of an enterprise environment can significantly change when a program (software) is updated; when a new hardware is added or removed; and when a security policy is added, changed or removed. Different approaches have been utilized to quantify the security of enterprise environments. In this section, we review previous research efforts related to security metrics such as attack graphs, the topological vulnerability analysis, IDS metrics, and security metric for unknown attacks. Some of these methodologies are discussed below.

2.6.1 Attack Graph

One of the most common methods used by many researchers to assess the security risk level of network is the attack graph [47]. This idea was first suggested as a supportive method to assist network administrators in measuring the security of a network based on security attributes and vulnerabilities. It focuses on the “attack-centric” view of the system [48]. An attack graph is considered appropriate if it is easy to understand and consumes less time in evaluating the vulnerabilities contained in a system, and also should be adaptive according to the system configuration [49].

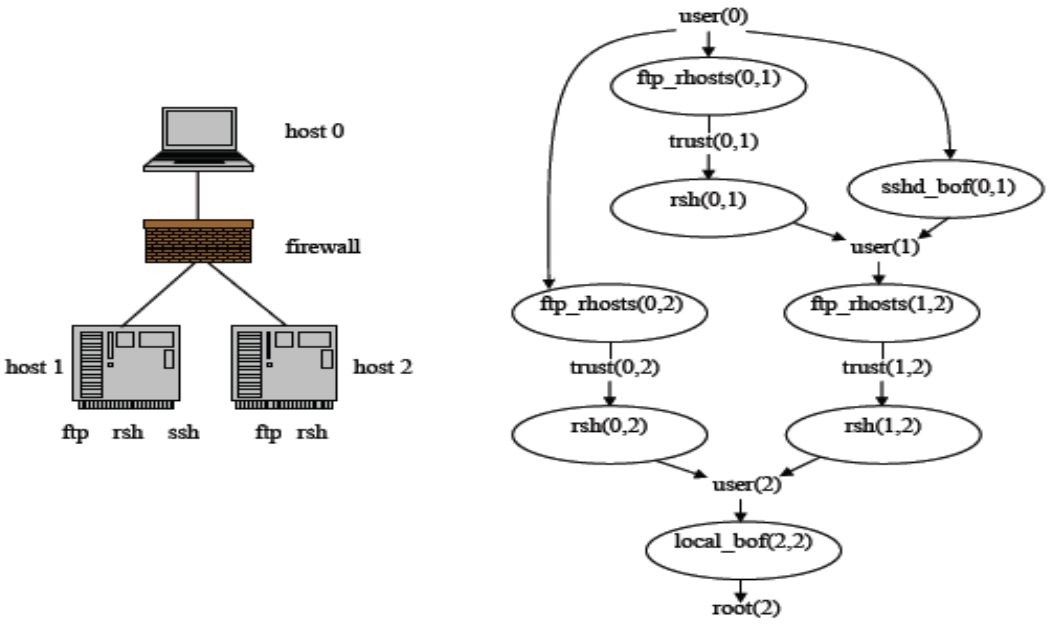

Figure 2.3: Attack graph [51].

The Figure 2.3 gives a simple example of a network structure with a corresponding attack graph, where file server (Host 1) is running file transfer protocol (ftp), secure shell (ssh) and remote shell (rsh) services, whereas, database server (Host 2) is running only ftp and rsh services. Firewalls is

introduced to filter the traffic from host 0 so that only ftp, ssh and rsh traffic is allowed to reach to the server side. In the attack graph on the right, the oval shapes represent the vulnerabilities and the texts inside the ovals show the conditions. The first and the second number in the parentheses indicate the source host number and destination host number respectively. The idea of attack graph was initiated by [50] who suggested that a system could be treated as a privilege graph exhibiting operational security vulnerabilities with each node represents a set of privileges owned by the user and each edge denotes vulnerabilities. A Markov model was then applied to those vulnerabilities in order to determine all possible paths that could be exploited by an attacker based on mean time to failure (MTTF) approach.

Failure to always be able to calculate the MTTF in even the smallest graphs led to [48] suggesting a new approach of using the optimal shortest path calculations to measure the system vulnerabilities. In their follow up work, [52] developed attack graph tool used three inputs: 1) the attack templates which define the capabilities and vulnerabilities of the system, 2) the configuration file which describes the system architecture, and 3) the attacker profile which defines the skills of the attacker. The attack graph was then constructed from the initial state using forward exploration method in order to provide all the possible paths that an attacker could take to compromise the system and the possible undesirable activities that the attacker could perform once inside the system.

Later, another approach called model checking approach was implemented as an input to the attack graph to assess the overall security of a network

based on interaction of the vulnerabilities, which could be identified with the help of various scanning tools such as System Scanner by ISS [53], Nessus [44] and CyberCop by Network Associates [54], etc. Ref. [55] incorporated unmodified model checker SMV approach in their work, but the problem with this technique is, it can obtain only one counter-example i.e., only one attack corresponds to an unsafe state. A service running on a single host can provide much better security than many services running on an individual host. This scheme can be applied to a variety of real-world problems like security, reactive system analysis, fault tolerance, operating systems, hardware design and protocol analysis [56]. The SecurlTree, a commercial threat risk assessment tool usually called capabilities-based attack tree analyser developed by [57] is easy to use threat risk analysing software package. It is widely used in defence and intelligence organization, nuclear power stations, health care providers, critical infrastructure companies, aerospace manufacturers, financial organizations, national laboratories and consulting companies. It shows all possible paths and set of resources that attacker can utilise to reach the desired target. After constructing the attack graph, the next step is to create descriptions of the goal and capabilities of each possible threat source. All the description is stored in threat agent profile which can be used and reused in different analyses. By using SecurlTree graphical interface, a network analyst can easily describe threats and system vulnerabilities.

Another approach to measuring security metrics was proposed by [58], where a new view of the attack graph construction was introduced. It was

argued that the main purpose of using attack graph was to represent pre and post-conditions of an exploit in the form of chain that could be used by security management to find out the ways through which attackers reached the desired target. Therefore, the attack graph was reintroduced as a state transition diagram in which each state indicates defender, attacker or system. Defender and system were related to action chosen by an attacker which led to changes in the overall state of the system. To produce and analyse this specific type of attack graph, model checking algorithm NuSMV and GraphViz visualization package had been utilized. In [59], they compared their work to [48] and it was found that Sheyner attack graph method was more general than [48]. Another disparity was noted in that Sheyner worked backwards from the goal state to construct the attack graph while Swiler constructed the attack graph starting from the initial state using the forward exploration algorithm. The backward algorithm saved the time by avoiding the exploration of the non-important paths in relation to a specific attack. However, the paths due to vulnerabilities irrelevant to the end goal may not be explored.

To analyse the security of enterprise network, it was necessary to figure out multi-stage and multi host attacks [11], [60]. Since, the configuration of one system affects the security of others in a network; security management is required to develop such attack graph tools, which should automatically identify the potential security vulnerabilities and configuration of a network. Then, the network administrator would be able to select appropriate countermeasures to prevent it from the possible malware attacks accordingly

[8]. In this regards, a network security analyser, multi-host, multi-stage vulnerability analysis language (MulVAL) was proposed to help the user in understanding the causal relationship between successful attacks and system configuration [61]. It takes output from VST to model possible attacks. It shows the logical associations among attack goals and configuration information based on logical programming [62], [63]. This graph has size polynomial to the network being evaluated. A node in the graph represents a logical statement, which does not specify the entire state of the network, but only a part of it, whereas, edges describe the causality relations between network configurations and an intruder's potential privileges [64]. A network security planning architecture (NetSPA) was another multiple prerequisite attack graph generating tool for security management to analyse thousands of vulnerabilities in a very short period of time [11]. This tool was incorporated to create network model by exploiting firewalls rules and network VST. This had the capability to report vulnerabilities having severe impacts on the network and to models zero day attacks by supposing that each software was vulnerable [47].

With the help of automated attack graph, it was possible to replicate high prone vulnerabilities with low impact vulnerabilities [65]. Further, it was claimed that a network with less number of vulnerabilities could offer better security as compared to the one with high number of vulnerabilities. To determine the possibility of future attacks, a method was proposed for generating network attack graph using data mining scheme based on DARPA 1999 and 2000 alerts datasets, generated from network intrusion

detection system (NIDS) [66]. As most of intrusion alerts achieved from the datasets might be of type false positives; therefore, it was difficult to determine which alerts were appropriate for evidence of intrusion prediction. An atomic domain was reported another simple and scalable attack graph generating approach, where the whole network was transformed into atomic domains representing the hosts with specific privileges but the work did not cater for overlapped vulnerabilities [67].

The work on Bayesian network (BN) was reported in [68] to model all possible atomic attack phases in a network. The same work was further explored by [51] and proposed a dynamic BN, which comprised sequence of variables considered as states of hidden Markov chain model having Markovian property in which the current state depends upon the previous state of the system. It is a graphical model for probabilistic inferences, which coordinates users to monitor and update the system with respect to time and also helps to predict further behaviour of the system or entire network. To make a secure network, it is necessary to measure its security based on different network configurations, i.e. topology, connectivity, etc. It was claimed that the proposed model efficiently described the security of an enterprise network. The BN was also implemented by [69] to generate attack graph using MulVAL tool to check whether the scheme was helpful in security analysis or not. In this approach, the BN used the information generated by IDS. Although these approaches provide ways to measure how vulnerabilities in a system can be exploited but they are unable to measure the absolute network security risk level quantitatively.

The topological vulnerability analysis (TVA) approach introduced by [70] showed all possible attack paths in a network based on node's individual and collaborative vulnerabilities. The attack graphs used the network vulnerabilities and the potential attacker profile to compute the overall security of the network. This approach had many advantages over many of its predecessors, for example, it provided the potential paths of vulnerability from which mitigation methods could be deduced, it employed algorithms that worked efficiently in big network setups. The TVA tool can also be used to generate an attack graph for 37000 vulnerabilities.

One of the biggest hindrances in securing a network is the zero-day attack that exploits system vulnerabilities. A novel security metric was proposed in [39] by counting the number of vulnerabilities required to compromise a network. This is an interesting work; however, it has some limitations such as the lack of vulnerability ranking, which we account for in this study.

2.7 Chapter Summary

This chapter provided an overview of different methods and tools that were explored during this study. Assessing the security risk at enterprise level is an essential step for network security communities now-a-days. Metrics are helpful tools for security analyst in identifying the security risk level within an organization as well as answering many security risk related questions. Network administrators are keen to attain a quantitative value rather than qualitative results. Various security metrics systems exist such as attack graphs but they do not provide the overall security risk level of the network.

Chapter 3.

QUANTITATIVE SECURITY RISK ASSESSMENT OF KNOWN ATTACKS

3.1 Introduction

In this chapter, a novel security metric is introduced which extends from common vulnerability scoring system (CVSS) to create an absolute value as the risk level of a system. The proposed methodology is applied to a computer network of an existing UK based organization with several departments. Nexpose [71] vulnerability scanning tool (VST) is incorporated to collect all vulnerabilities from the network. On the basis of CVSS standards, the vulnerabilities are classified into one of three possible levels: critical, severe and moderate. The security risk level of each department is computed using probability theory on VST data. In addition, the overall security risk level of the entire network is also computed. The purpose of these metrics is to facilitate the network administrator a valuable way to assess the security risk level quantitatively.

3.2 Common Vulnerability Scoring Systems (CVSS)

Vulnerability assessment plays an important role for security posture and risk management. To measure the severity level of vulnerability, there is a need of well-defined security metrics which should be based on scientific evidence, systematic and quantitative approaches. The CVSS provides a tool to quantify the severity and risk of a vulnerability to an information asset in an IT environment [47]. The reason for selecting CVSS in our experiments

is four fold: 1) it is a completely free open source standard, 2) it provides a prioritized framework, 3)it helps in scoring IT security vulnerabilities, 4) it is globally accepted and adopted by the industry. This standard was first launched by National Infrastructure Advisory Council (NIAC) in July 2003 and the latest version (CVSS-3) works under the supervision of the Forum of Incident Response Teams (FIRST). The CVSS facilitates the user with a composite score by means of vulnerability showing the overall severity and security risk of a system. It is a useful language especially designed for application vendors, researchers, IT managers and vulnerability bulletin providers [72]. It is generally composed of three metric groups: base, temporal and environmental, each consisting of a set of metrics. All these metrics generate a numeric value in the range from 0 to 10. These metric groups are discussed in the following sections.

3.2.1 Base Metrics

The base metric group expresses the characteristics of vulnerability, which are constants with respect to time and user environments. Figure 3.1classifies the base metrics into two categories: access metrics and impact metrics. Access metrics includes vector, complexity and authentication which show how the vulnerability is accessed and whether or not extra conditions are required to exploit it, whereas, impact metrics contain confidentiality, integrity and availability which measure how exploited vulnerability can directly affect IT assets [73], [74].Figure 3.2 depicts a screenshot sample of CVSS base scoring calculator used to determine the base score of vulnerability. If vulnerability has no impact on confidentiality, integrity and

availability, then base score is zero. The base metrics results are further utilized in calculating temporal scores of temporal metrics.

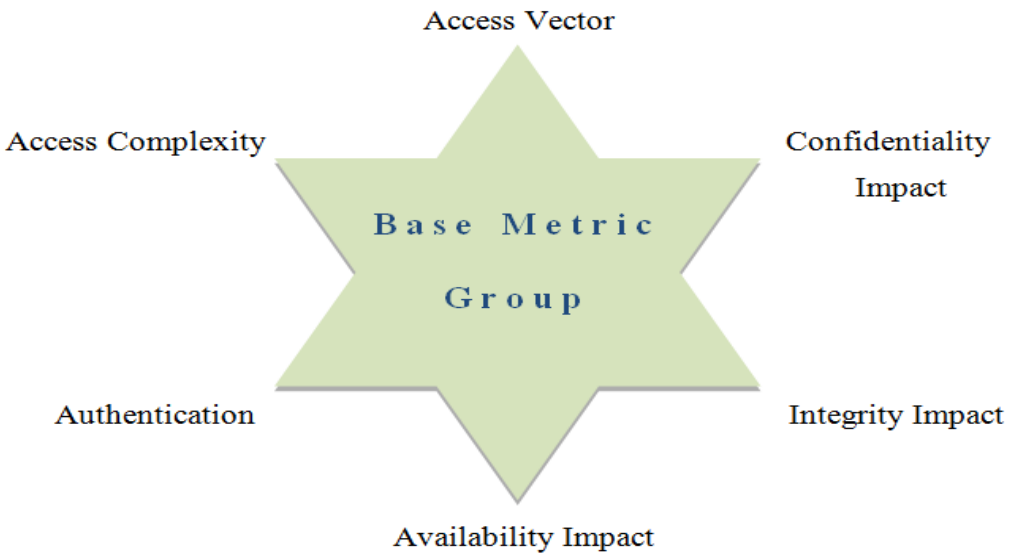

Figure 3.1: The Base metric group.

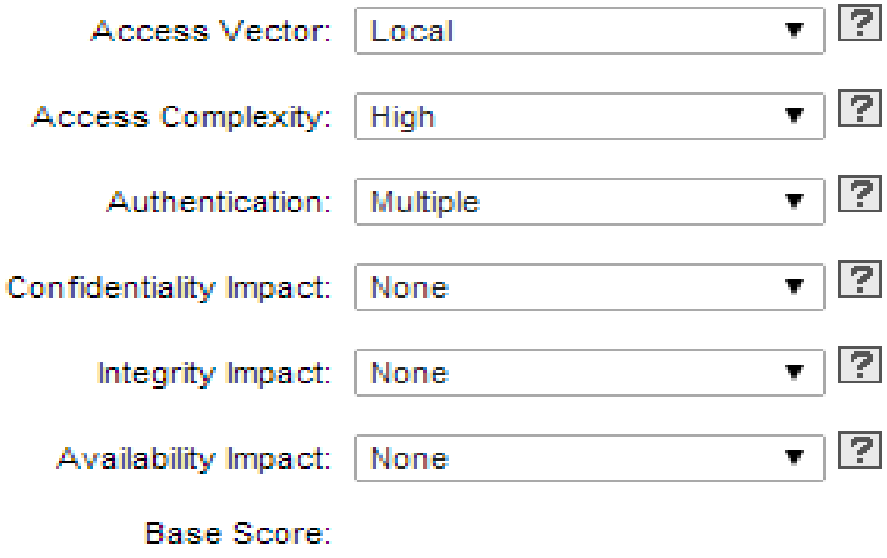

Figure 3.2: Base metric screenshot.

3.2.2 Temporal Metrics

This metrics group represents the characteristics of time dependent vulnerability. The factors involved in calculating the metrics are exploitability, remediation level and report confidence as shown in Figure 3.3. The exploitability depends upon the exploiting technology as well as the tools availability. It identifies the current status of the exploited technique or code availability. If code is accessible and easy to use, then severity risk level of vulnerability will be high. If vulnerability becomes common, the risk of attack will become high eventually leading to increase in temporal metrics score.

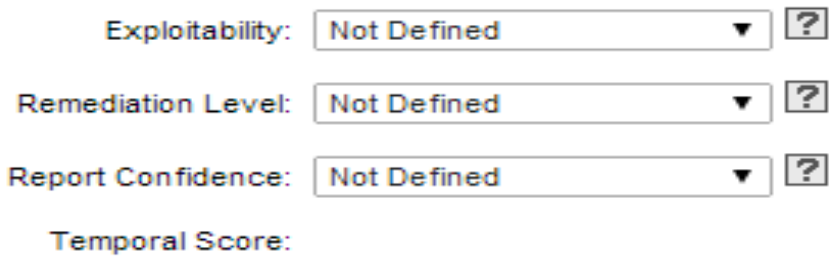

Figure 3.3: Temporal metric screenshot.

Remediation level investigates the severity level of vulnerability in terms of its remediation like temporary fix or official fix. The temporal score of vulnerability increases if it is not officially patched. The report confidence measures the degree of confidence in the presence of known vulnerability and credible technical details.

3.2.3 Environmental Metrics

Environmental metrics group captures those vulnerability characteristics that are uniquely associated with a particular user's IT environment. This group

uses base and current temporal scores to assess the severity risk level of vulnerability in the context of the way that the vulnerable product or software is deployed. Figure 3.4 classifies the Environmental metrics into two main categories; collateral damage potential and target distribution, along with three other security requirements. Collateral damage measures the potential for a loss of physical equipment, property damage or loss of life and target distribution measures the relative size of the field of target system susceptible to the vulnerability. The three security requirements; confidentiality, integrity and availability allow the environmental score to be fine-tuned according to the user's environment.

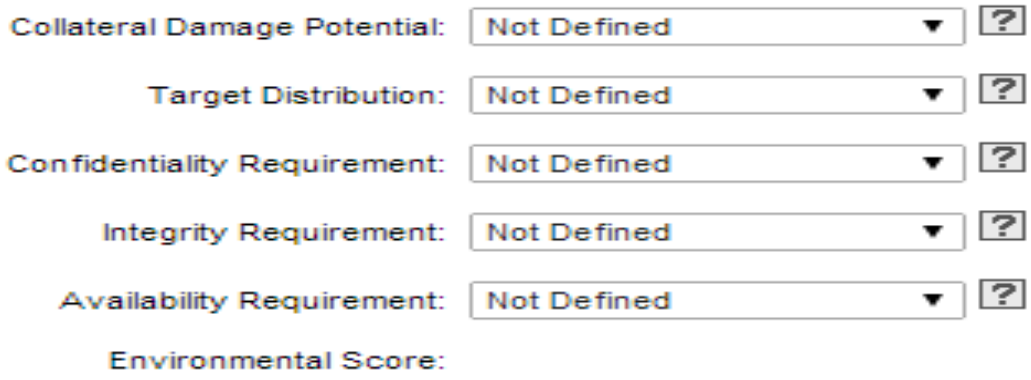

Figure 3.4: Environmental metric screenshot.

3.3 Proposed Approach

Quantifying the level of network security has become a challenging problem especially for an enterprise environment [75], [76]. Various commercial and non-commercial tools have been introduced in the literature employed by network administrators to assess the security risk levels of their networks [77].These tools provide only fuzzy quantification of security risk level in terms of high, medium and low. This makes it hard for a network

administrator to know the level of risk associated with the network. However, there is a need for a new quantitative security metrics which should provide an absolute value of the overall security risk level of a network. The enterprise network structure can be broken down into the smallest network resources in order to measure the security risk generated by known vulnerabilities. This is the approach used in the design of this methodology.

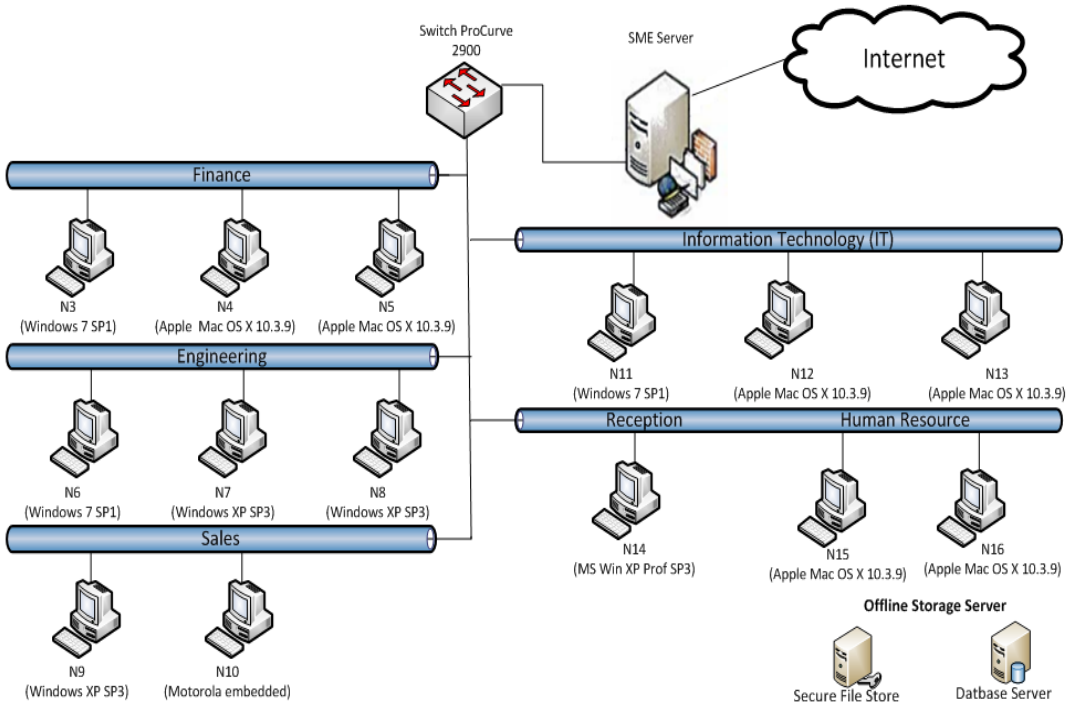

Figure 3.5: Network diagram.

The enterprise network is divided into departmental networks and, which in turn are further subdivided into network nodes. The different vulnerabilities are taken into account and then, by using different probabilistic approaches, a metric is designed based on known attacks providing security risk assessment level of the respective network.

3.3.1 Test Bench

In order to measure security risk level of enterprise networks based on known vulnerabilities, a UK based company containing 16 nodes and a switch. The company infrastructure design and operating systems installed on nodes are illustrated in Figure 3.5. As shown, the network setup consisting of 16 nodes is connected through the ProCurve Series 2900 switch to the SME server, which is responsible for monitoring all incoming and outgoing traffic. A list of all vulnerabilities in the network is collected by deploying Nexpose VST. After running full scan, 1777 vulnerabilities of different types have been discovered and are listed in appendix A.

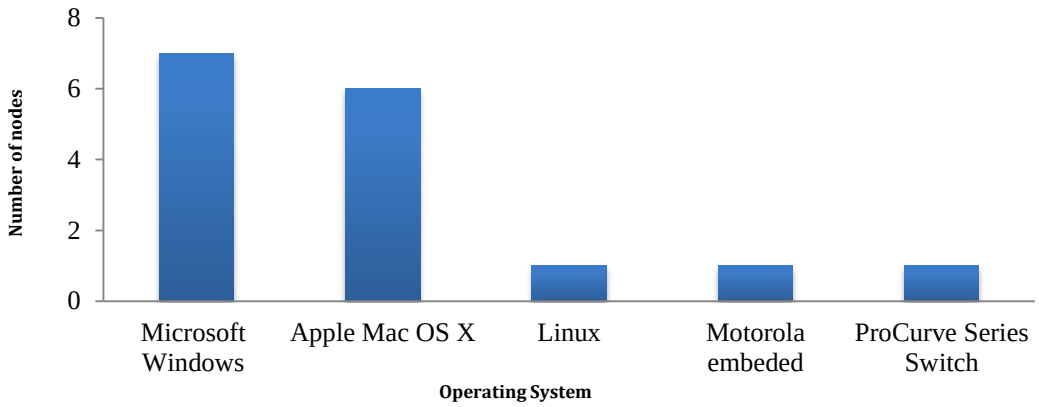

Figure 3.6: Distributions of operating systems.

Figure 3.6 shows the number of nodes running on different operating systems at the time of vulnerability scanning. Five operating systems are employed in which Microsoft Windows XP Professional SP3 on seven nodes, Apple Mac on six nodes, Linux, Motorola embedded and ProCurve Series Switch on one node each.

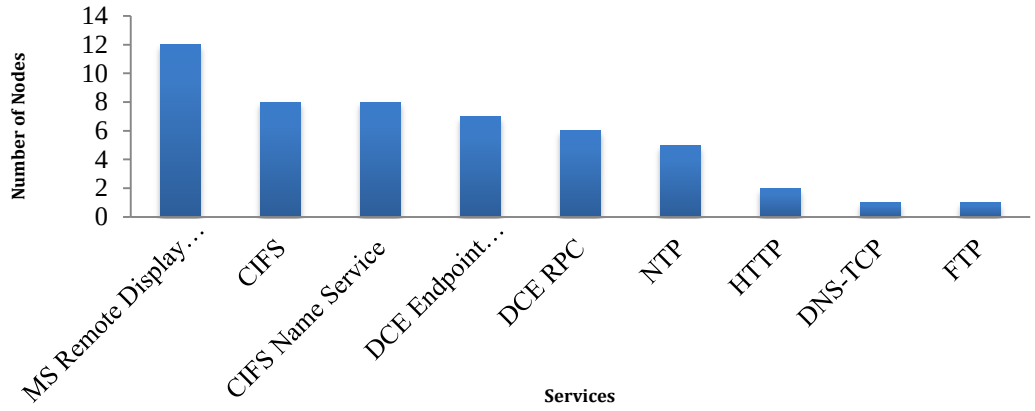

Figure 3.7: The number of nodes vs. different services.

Figure 3.7 shows different services provided by operating systems running on the network. During scanning, it is found that 23 services are operated. Out of which Microsoft Remote Display Protocol (MS-RDP) service is running on 12 nodes, Common Internet File System (CIFS) service is on 8 nodes and so on.

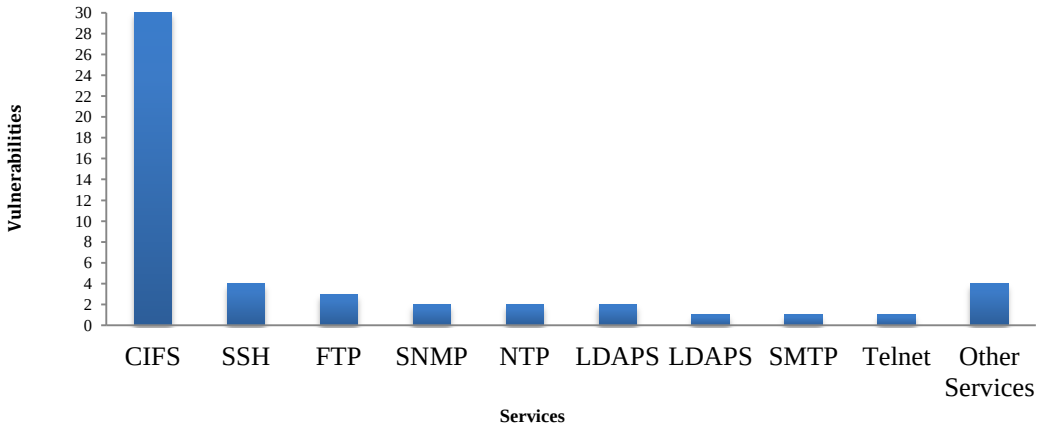

Figure 3.8: The number of vulnerabilities related to each of the services.

Figure 3.8 illustrates that CIFS service is most vulnerable to attacks because it contains higher number of vulnerabilities as compared to other services.

Note that CIFS is a standard protocol that allows computer users to share files across intranet as well as the Internet.

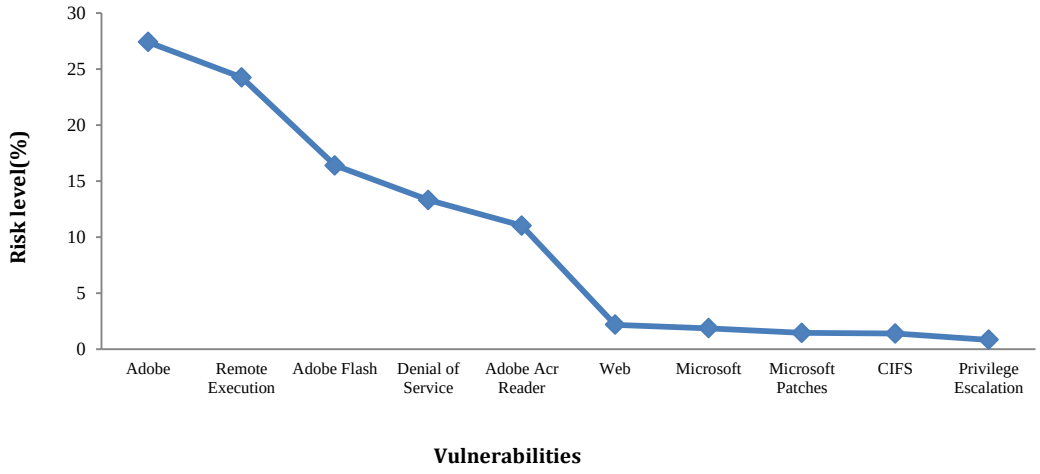

Figure 3.9: Most common vulnerabilities categories by percentage (%).

During the scan, 1592 vulnerabilities were found related to the Adobe category making the network the most susceptible to attacks. The adobe-reader-APSB12-16-cve-2012-2049, windows-hotfix-ms12-078, adobe-apsb12-22-cve-2012-5262, adobe-flash-apsb13-05-cve-2013-0638, adobe-apsb12-07-cve-2012-0773, adobe-reader-apsb12-08-cve-2012-0775, adobe-reader-apsb12-08-cve-2012-0774, adobe-reader-apsb12-08-cve-2012-0776, adobe-apsb11-28-cve-2011-2450 and adobe-reader-apsb13-02-cve-2013-0612 are the vulnerabilities, which pose the highest risk to the organization as shown in the appendix A. By using the temporal metric from CVSS standard, vulnerability risk scores are calculated based on the likelihood of attack as well as the effects associated with a successful attack. The achieved scores are then multiplied by the number of instances of the vulnerability on the network to come up with the final risk score.

3.3.2 Vulnerability Classifications by Severity Risk Level

The list of vulnerabilities classified according to CVSS standard is shown in Table 3.1.

Table 3.1: Nodes by vulnerability severity.

Nodes	Operating Systems	Critical	Severe	Moderate
N1	Linux 2.6.18-308.24.1.e15	2	12	8
N2	ProCurve Series 2900 Switch	2	-	2
N3	Microsoft Windows 7 professional Edition SP1	-	2	-
N4	Apple Mac OS X 10.3.9	-	-	-
N5	Apple Mac OS X 10.3.9	-	-	-
N6	Microsoft Windows 7 Professional Edition SP1	-	2	-
N7	Microsoft Windows XP Professional SP3	365	68	3
N8	Microsoft Windows XP Professional SP3	365	68	3
N9	Microsoft Windows XP Professional SP3	365	68	3
N10	Motorola embedded	-	-	1
N11	Microsoft Windows 7 Professional Edition SP1	-	2	-

N12	Apple Mac OS X 10.3.9	-	-	-
N13	Apple Mac OS X 10.3.9	-	-	-
N14	Microsoft Windows XP Professional SP3	365	68	3
N15	Apple Mac OS X 10.3.9	-	-	-
N16	Apple Mac OS X 10.3.9	-	-	-

It is clear from Table 3.1 that the total vulnerabilities collected through Nexpose VST are 1777. Some of them are having high-impact while others have either medium-impact or low-impact on the company's network.

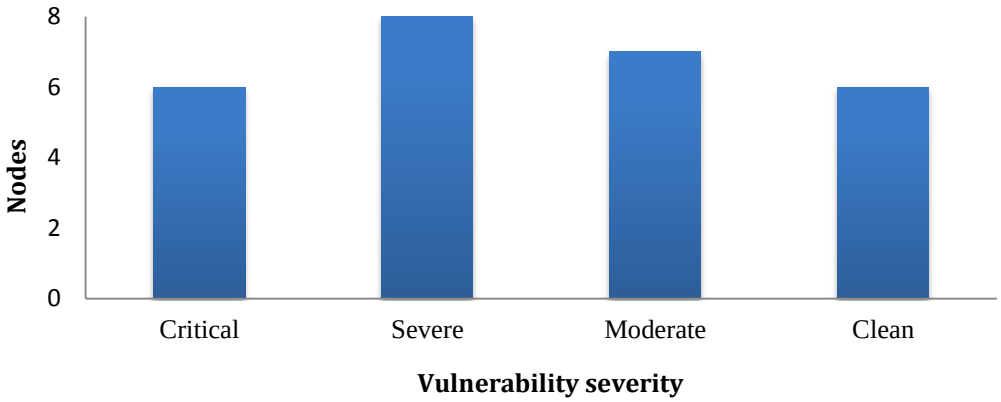

Figure 3.10: Nodes by vulnerability severity

Figure 3.10 shows the distribution of vulnerabilities over different nodes. It can be observed that six nodes contain critical vulnerabilities, eight nodes having severe vulnerabilities and seven nodes comprise moderate vulnerabilities, whereas the remaining six nodes are free from any vulnerability.

3.4 Results and Discussions

Three scenarios are constructed which quantitatively assess the security risk level of the existing UK company network in terms of absolute value. Let critical, severe and moderate vulnerability be represented by C, S and M respectively. Suppose Ni represents the i^{th} node in the network, then security risk level of each department and entire network can be computed with respect to all vulnerabilities, and individual vulnerabilities in terms of *C*, *S* and *M*. The scenarios are divided into following three:

- Scenario-I details the method of calculating the probability of attack on each department in terms of *C*, *S* and *M*.
- Scenario-II provides the method of calculating the probability of attack on each department in terms of total known vulnerabilities.
- Scenario-III provides the method of calculating the probability of attack on company network.

3.4.1 Scenario-I

In this section, the probability of attack on IT (P_{IT}), Finance (P_{Fin}), Sales (P_S), Engineering $(P_{ENG})$and Human Resource (P_{HR}) departments with respect to critical, severe and moderate vulnerability is calculated. These probabilities are determined using total law of probability as detailed below:

$$P_{Fin}(C) = \sum_{i=3}^{5} P(N_i \cap C) \tag{3.1}$$

$$P_{Fin}(C) = \sum_{i=3}^{5} P(N_i)P(C/N_i)$$

$$P_{Fin}(C) = P(N_3 \cap C) + P(N_4 \cap C) + P(N_5 \cap C)$$

$$P_{Fin}(C) = P(N_3)P(C/N_3) + P(N_4)P(C/N_4) + P(N_5)P(C/N_5)$$

Now, using Table 3.1,

$$P_{Fin}(C) = \frac{1}{3}.\frac{0}{2} + \frac{1}{3}.\frac{0}{0} + \frac{1}{3}.\frac{0}{0}$$

$$\Rightarrow P_{Fin}(C) = 0 \tag{3.2}$$

Similarly,

$$P_{Fin}(S) = \sum_{i=3}^{5} P(N_i \cap S) = 33\% \tag{3.3}$$

$$P_{Fin}(M) = \sum_{i=3}^{5} P(N_i \cap M) = 0 \tag{3.4}$$

$$P_{ENG}(C) = \sum_{i=6}^{8} P(N_i \cap C) = 55.7\% \tag{3.5}$$

$$P_{ENG}(S) = \sum_{i=6}^{8} P(N_i \cap S) = 43.7\% \tag{3.6}$$

$$P_{ENG}(M) = \sum_{i=6}^{8} P(N_i \cap M) = 0.4\% \tag{3.7}$$

$$P_S(C) = \sum_{i=9}^{10} P(N_i \cap C) = 41.8\% \tag{3.8}$$

$$P_S(S) = \sum_{i=9}^{10} P(N_i \cap S) = 7.8\% \tag{3.9}$$

$$P_S(M) = \sum_{i=9}^{10} P(N_i \cap M) = 50.3\% \tag{3.10}$$

$$P_{IT}(C) = \sum_{i=11}^{13} P(N_i \cap C) = 0 \tag{3.11}$$

$$P_{IT}(S) = \sum_{i=11}^{13} P(N_i \cap S) = 33.3\% \tag{3.12}$$

$$P_{IT}(M) = \sum_{i=11}^{13} P(N_i \cap M) = 0 \tag{3.13}$$

$$P_{HR}(C) = \sum_{i=15}^{16} P(N_i \cap C) = 0 \tag{3.14}$$

$$P_{HR}(S) = \sum_{i=15}^{16} P(N_i \cap S) = 0 \tag{3.15}$$

$$P_{HR}(M) = \sum_{i=15}^{16} P(N_i \cap M) = 0 \tag{3.16}$$

Since there is no critical (*C*) or moderate (*M*) vulnerability found in Finance department, therefore, this department is 100% secure in terms of critical and moderate known vulnerability as shown in Eq(3.2) and Eq(3.4). From Eq(3.3), the security risk level with respect to severe vulnerability is 33%, which implies that the Finance department is 67% secure according to known vulnerabilities. From Eqs 3.5-3.7, the Engineering department is 44.3% secure in terms of critical vulnerability, 56.3% secure in case of

severe vulnerability and 99.6% secure with respect to moderate vulnerability. Now, from Eqs 3.8-3.10, it is clear that the Sales department is 58.2% secure in terms of critical vulnerability, 92.2% secure in case of severe vulnerability and 49.7% secure with respect to moderate vulnerability. From Eqs 3.11-3.13, it is noted that there is no *C* or *M* exists in the IT department, therefore, this department is fully secure in terms of critical and moderate vulnerabilities. The only vulnerability found is S; due to this, the department is 67% secure. Finally, since there are no vulnerabilities found in the HR department, this department is 100% secure in terms of all vulnerabilities as is evident from Eqs 3.14-3.16.

3.4.2 Scenario-II

The next step is to calculate the security risk level of attacks on each department with respect to total vulnerabilities. These probabilities are calculated using inclusion-exclusion principle of probability. By using the same notation as in the previous scenario, the probability of attack on the finance department ($P(Fin)$) is calculated by

$$P(Fin) = \sum_{K=3}^{5} (-1)^{K+1} \left(\sum_{3 \le i_3 < i_4 < i_5 \le 5} P\left(N_{i_3} \cap N_{i_4} \cap N_{i_5}\right) \right) \tag{3.17}$$

Where the value of K and i is the position of the node in the department network as shown in Figure 3.5.

$$= (-1)^{3+1} \sum_{3 \le i_3 \le 5} P\left(N_{i_3}\right) + (-1)^{4+1} \sum_{3 \le i_3 < i_4 \le 5} P\left(N_{i_3} \cap N_{i_4}\right)$$

$$+ (-1)^{5+1} \sum_{3 \le i_3 < i_4 < i_5 \le 5} P\left(N_{i_3} \cap N_{i_4} \cap N_{i_5}\right)$$

$$= \sum_{3\le i_3\le 5} P(N_{i_3}) - \sum_{3\le i_3<i_4\le 5} P(N_{i_3}\cap N_{i_4}) + \sum_{3\le i_3<i_4<i_5\le 5} P(N_{i_3}\cap N_{i_4}\cap N_{i_5})$$

$$= P(N_3) + P(N_4) + P(N_5) - P(N_3\cap N_4) - P(N_4\cap N_5) - P(N_3\cap N_5) + P(N_3\cap N_4\cap N_5)$$

$$\Rightarrow P(Fin) = 0.1\% \tag{3.18}$$

$$P(Eng) = \sum_{K=6}^{8}(-1)^{K+1}\left(\sum_{6\le i_6<i_7<i_8\le 8} P(N_{i_6}\cap N_{i_7}\cap N_{i_8})\right) \tag{3.19}$$

$$= \sum_{6\le i_6\le 8} P(N_{i_6}) - \sum_{6\le i_6<i_7\le 8} P(N_{i_6}\cap N_{i_7}) + \sum_{6\le i_6<i_7<i_8\le 8} P(N_{i_6}\cap N_{i_7}\cap N_{i_8})$$

$$= P(N_6) + P(N_7) + P(N_8) - P(N_6\cap N_7) - P(N_7\cap N_8) - P(N_6\cap N_8) + P(N_6\cap N_7\cap N_8)$$

$$P(Eng) = 24.5\% \tag{3.20}$$

$$P(Sales) = \sum_{K=9}^{10}(-1)^{K+1}\left(\sum_{9\le i_9<i_{10}\le 10} P(N_{i_9}\cap N_{i_{10}})\right) \tag{3.21}$$

$$= \sum_{9\le i_9\le 10} P(N_{i_9}) - \sum_{9\le i_9<i_{10}\le 10} P(N_{i_9}\cap N_{i_{10}})$$

$$= P(N_9) + P(N_{10}) - P(N_9\cap N_{10})$$

$$P(Sales) = 24.6\% \tag{3.22}$$

$$P(IT) = \sum_{K=11}^{13}(-1)^{K+1}\left(\sum_{11\le i_{11}<i_{12}<i_{13}\le 13} P(N_{i_{11}}\cap N_{i_{12}}\cap N_{i_{13}})\right) \tag{3.23}$$

$$= \sum_{11 \le i_{11} \le 13} P(N_{i_{11}}) - \sum_{11 \le i_{11} < i_{12} \le 13} P(N_{i_{11}} \cap N_{i_{12}}) + \sum_{11 \le i_{11} < i_{12} < i_{13} \le 13} P(N_{i_{11}} \cap N_{i_{12}} \cap N_{i_{13}})$$

$$= P(N_{11}) + P(N_{12}) + P(N_{13}) - P(N_{11} \cap N_{12}) - P(N_{12} \cap N_{13}) - P(N_{11} \cap N_{13}) + P(N_{11} \cap N_{12} \cap N_{13})$$

$$P(IT) = 0.1\% \tag{3.24}$$

$$P(HR) = \sum_{K=15}^{16} (-1)^{K+1} \left(\sum_{15 \le i_{15} < i_{16} \le 16} P(N_{i_{15}} \cap N_{i_{16}}) \right) \tag{3.25}$$

$$= \sum_{15 \le i_{15} \le 16} P(N_{i_{15}}) - \sum_{15 \le i_{15} < i_{16} \le 16} P(N_{i_{15}} \cap N_{i_{16}})$$

$$= P(N_{15}) + P(N_{16}) - P(N_{15} \cap N_{16})$$

$$P(HR) = 0 \tag{3.26}$$

The security risk level of each department in terms of total vulnerabilities is demonstrated in Figure 3.11.

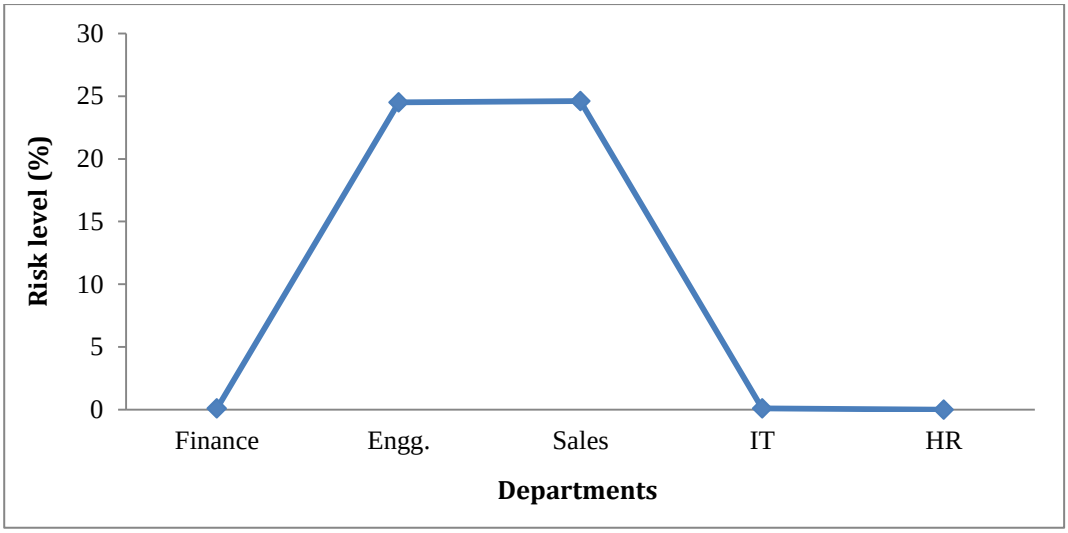

Figure 3.11: Department wise security risk levels.

Finance and IT departments have the same security risk level i.e. 0.1%, which implies that these departments are 99.9% secure. The security risk levels of Engineering and Sales department are almost the same with a difference of 0.1%. Since no vulnerability is found in HR department during the scan, therefore, the department is 100% secure.

3.4.3 Scenario-III

After calculating departmental security risk levels, the inclusion-exclusion principle of probability is also employed to calculate the company network security risk level with respect to total known vulnerabilities. Let $P(N)$ be the probability of attack on the entire network, then by inclusion-exclusion principle, we have:

$$P(N) = \sum_{K=1}^{16} (-1)^{K+1} \left(\sum_{1 \le i_1 < i_2 \ldots < i_K \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_K}\right) \right) (3.27)$$

$$P(N) = \sum_{1 \le i_1 \le 16} P\left(N_{i_1}\right) - \sum_{1 \le i_1 < i_2 \le 16} P\left(N_{i_1} \cap N_{i_2}\right) + \sum_{1 \le i_1 < i_2 < i_3 \le 16} P\left(N_{i_1} \cap N_{i_2} \cap N_{i_3}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_4 \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_4}\right) + \sum_{1 \le i_1 < i_2 \ldots\ldots < i_5 \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_5}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_6 \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_6}\right) + \sum_{1 \le i_1 < i_2 \ldots\ldots < i_7 \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_7}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_8 \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_8}\right) + \sum_{1 \le i_1 < i_2 \ldots\ldots < i_9 \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_9}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{10} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{10}}\right) + \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{11} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{11}}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{12} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{12}}\right) + \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{13} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{13}}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{14} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{14}}\right) + \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{15} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{15}}\right)$$

$$- \sum_{1 \le i_1 < i_2 \ldots\ldots < i_{16} \le 16} P\left(N_{i_1} \cap N_{i_2} \ldots \cap N_{i_{16}}\right)$$

After expanding Eq(3.27) and using Table 3.1, for probabilistic values;

$$P(N) = 28.9\% \tag{3.28}$$

This shows that the security risk level on company's entire IT network is 28.9%, which implies that the network is 71.1% secure.

3.5 Conclusion

This chapter discussed the proposed methodology used to quantify the security risk levels of any enterprise IT network. The method was designed using a case study of a UK company, which was electronically scanned by Nexpose VST to identify the vulnerability level. The vulnerabilities were then classified according to CVSS standard (critical, severe and moderate).

Probability theory was applied to calculate the overall security risk level for each department and the entire network. The work done in this chapter used the known vulnerabilities acquiring from the network as the prime factor for calculating the risk metrics. These metrics are valuable for any network administrator to acquire an absolute risk assessment value. In next chapter, unknown vulnerabilities and human factors will be considered as a source of vulnerabilities that may affect the security risk level of a company.

Chapter 4.

RISK METRICS FOR INVISIBLE ATTACKS

4.1 Introduction

Today, information systems that are commonly used can be abused to exploit network vulnerabilities. One of such systems is the Google search engine. Given the increasing dependence of our societies on networked information systems, the level of sophistication of cyber attacks that target to compromise enterprise networks have risen a great deal in the last decade. These attacks have evolved thereby making it increasingly challenging to differentiate between legitimate and illegitimate traffic. Cybercrimes are a great threat to the enterprise networks because in most cases severity of the threat is not known until it is too late. This is due to many factors such as inadequate skilled network administrators and, lack of collaboration between the authorities, the computing companies and the research communities [78], [79]. Currently, despite the efforts being provided by security communities to secure networks, a strong sense of insecurity still prevails. This calls for creation and development of new methods to counter cyber attacks that can cause businesses to fail [80].

At any time, a network system has much vulnerability which involves in many factors such as human factor, known and unknown vulnerabilities, etc. These vulnerabilities are exploited during attacks. Unknown vulnerabilities create a huge challenge in the network due to its invisibility to the security measures

setting up in the system. Consequently, these vulnerabilities lead to invisible attacks, which can create traffic treated as a normal or legitimate in a network. In this chapter, a new way of looking at attacks based on visibility to the security setup is proposed. Here, those attacks are considered which target the critical infrastructure of the information and business networks [79].

To clearly understand the steps involved in assessing the security risk level of an enterprise network, attacks are categorised into four different levels of visibility. The emphasis of this study is on one level of attacks known as the invisible attacks. One of the major source of these attacks is the Google dorks which lists all the information it finds on the networks including sensitive information that can be exploited by intruders [81], [82].This attack is usually seen as genuine traffic to the network security setup posing a challenge for which a countermeasure is required. Based on the analysis, a method for detecting and preventing invisible attacks is proposed. Furthermore, open web application security project (OWASP) risk rating methodology is applied on the enterprise network to assess the overall severity risk level of the invisible attacks. This method basically provides severity risk level in terms of high, medium and low which are not quantitative values, therefore, severity risk assessment table is incorporated to enable the retrieval of the quantitative risk value.

4.2 Visibility of Attacks: An Overview

Based on visibility on the system, attacks can be classified into the following four categories:

- Visible attacks

This category is composed of those attacks, which are visible to network security systems comprising well defined signatures database of known attacks. The signature based techniques also called knowledge based techniques are then applied to match the pattern of attack with the signatures database. If any pattern is matched, the network security system will generate an alert against the security violation.

- Visible behaviour

This category typically consists of those attacks that can be detected and prevented by well configured security countermeasures. These countermeasures observe the traffic and compare its pattern with the base line, and identify the norm for the network by performing activities like bandwidth inspection, protocol examination and ports evaluation. During packet filtration, if any suspicious traffic behaviour is found, the security countermeasures will generate an alert against it.

- Visible inside the host

This type of attacks is partially carried out inside the local system. Some rootkit or malware requires a restart after installation. Rebooting the system can be visible within the local host, but not on a network level. Malware generally performs modifications on system files; therefore, it is necessary to have a full picture of the attack to understand the changes made on local systems.

- Invisible attacks

In this category, attacker actions are generally considered as legitimate actions, therefore, this type of attack is not concerned for network security systems. For instance, a computer sends information out to another computer. This is a completely legitimate action. However, sending data from one computer to another may not be considered as a legitimate if the previous action is a brute force attack on root passwords. One of the prominent invisible attacks is the Google dork which is discussed in the following Section.

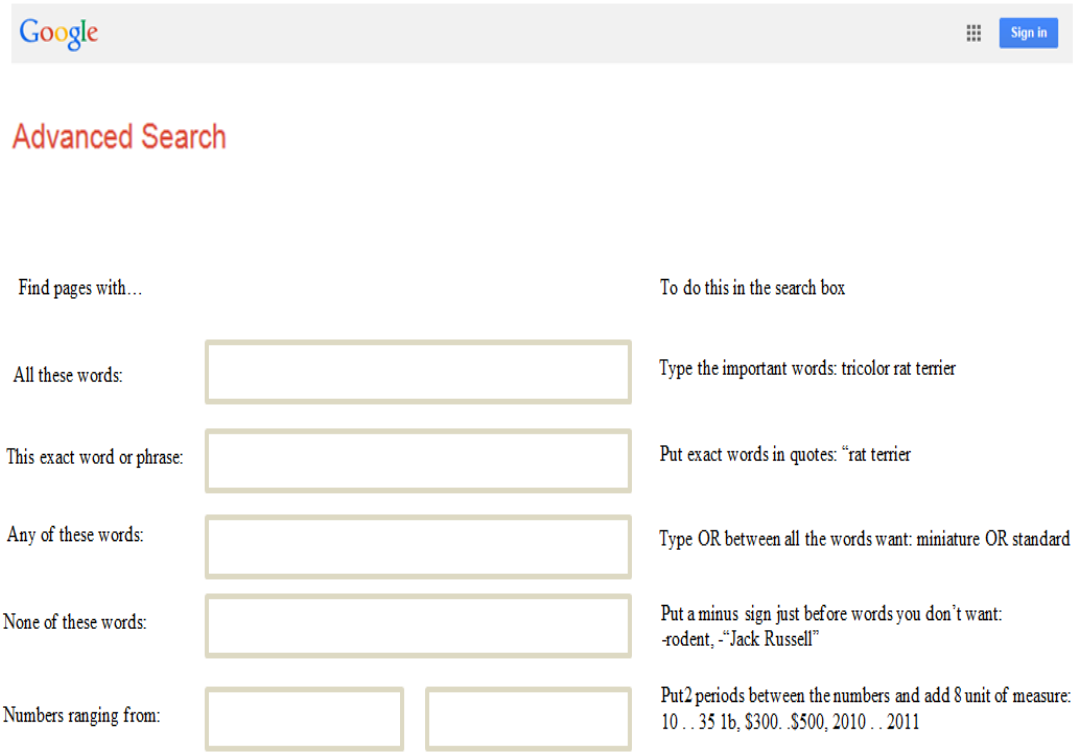

Figure 4.1Google advanced search.

4.2.1 Google Dorks

These are the commands being utilized to search necessary information about companies, can help the intruders to build a profile of their targets [81], [83]. It is a type of social engineering attack in which the attacker uses

Google advanced search engine shown in Figure 4.1 to collect sensitive information about the target.

Due to poor systems configuration, search engines gather more information than required while crawling the web using search operators. Table 4.1 provides a list of possible operators for different search services that can be used by intruders to generate invisible attack.

Table 4.1: Google search operators.

Search Service	**Search Operators**
Web Search	filetype, allinanchor, inanchor, site, intext, intext, inurl, related, allintext, allintitle, allinurl, cache, define, id, info, intitle, phonebook.
News	intext, intitle, inurl, allintitle, allintext, source, allinurl, location.
Groups	intext, allintext, author, allintitle, intitle, insubject, group.
Product Search	allintitle, allintext
Image Search	site, allinurl, allintitle, intitle, filetype, inurl,
Directory	filetype, ext, allintext, intext, inurl, intitle, allintitle, allinurl

Now-a-days, many search engines like Google have been used as hacking tools and this is becoming a critical challenge for network security communities to secure their information against invisible attacks, as most of the security countermeasures do not take this attack into account.

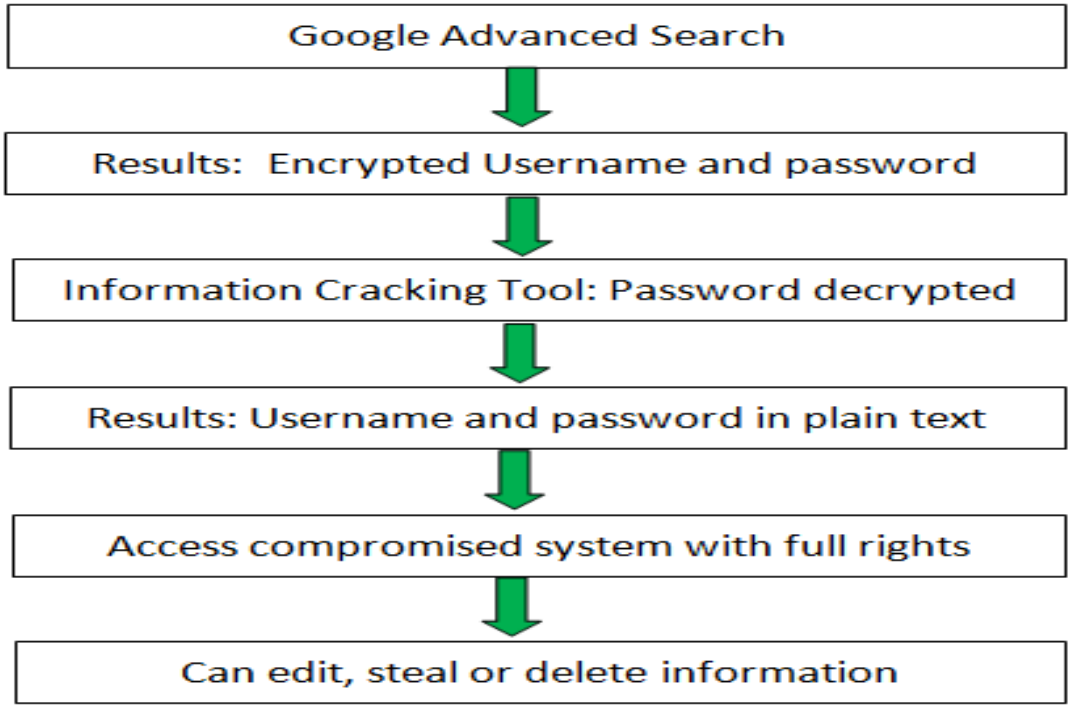

Figure 4.2Google attack scenario.

A particular attack scenario using search engine properties is illustrated in Figure 4.2, which shows that how a well written query in Google advanced search engine can be used to retrieve sensitive information such as usernames and passwords. The achieved information can be decrypted quickly using readily available cracking tools and further can be utilized in generating attacks. The system will treat this illegitimate user as a legitimate one and therefore, the employed security countermeasures on the network will be rendered useless.

4.2.1.1 Types of Invisible Attacks

Vulnerabilities exposed by search engines has been growing rapidly, therefore, there is a need to analyse them specifically. Based on their

characteristics, invisible attacks are classified into 9 groups given in Table 4.2.

Table 4.2: Google hacking database categories.

No.	Attacks	Number of commands
1	Files containing username and passwords in clear text	30
2	Files containing username and passwords in encrypted form.	21
3	Already login websites	4
4	Error code message (404)	7
5	Blogs / Forums	33
6	Pages contain login portal	116
7	Sensitive directories or files containing juicy information	134
8	Vulnerable information	129
9	List of emails	2

4.3 Proposed Approach

Security metrics are considered effective techniques to measure the extent to which an organization meets its security objectives. Conventional security metrics generally focus on qualitative risk assessment of known attacks and

vulnerabilities. Most of them utterly ignore the presence of invisible attacks in evaluating the overall security risk assessment of IT networks. The proposed methodology deals with invisible attacks like Google dorks and provides a way of detecting and preventing networks, and also assesses the network security risk from these attacks. To use the methodology, a list of Google dork commands are constructed (detail is given in Appendix B) and, are analysed and categorised in Table 4.1 and Table 4.2 respectively. The proposed scheme is composed of two scenarios and its effectiveness is evaluated using UK based company. In first scenario, a generic NIDS rule is constructed to monitor and protect the company network against invisible attacks. In second scenario, OWASP tool is incorporated to assess the security risk level affected by these attacks.

4.3.1 Test Bench

The under consideration company consists of Finance, Engineering, Sales, Information Technology and Human Resource departments as shown in Figure 4.3.The data of each department is restricted to those who work within that department. The company has its own web server through which all communications to and from the outside world take place. It is important to note that the company is unaware of invisible attacks due to insufficient knowledge. Signature based NIDP system is deployed in between firewall and web server to protect company sensitive information as it has the capability of detecting and preventing it from malicious intrusion by having a deep inspection of data packets.

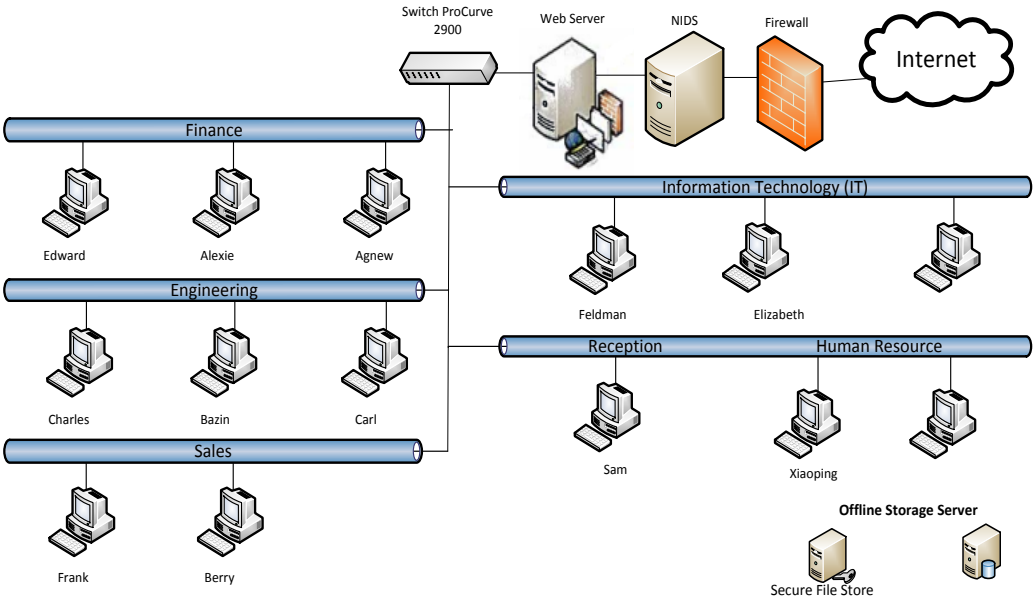

Figure 4.3: Network diagram.

4.3.2 Results and Discussion

To identify and quantify the security risk level against invisible attacks, two different scenarios are developed for the UK based company's network. These scenarios will investigate the two different areas of interest.

4.3.2.1 Scenario-I

In this scenario, one of the solutions of detecting and mitigating the risk of invisible attacks on the company network is discussed. Several Google dork commands have been generated using Google advanced search engine. It is found that confidential information of Sale department can be disclosed by Google dorks. The retrieved data contains important information such as employees' username, passwords, contact details, etc. To protect the Sale department data from Google dorks, signature based NIDP system is deployed in between firewall and web server as shown in Figure 4.3. The

basic purpose of firewalls is to block access to specific services by acting as security personnel at the network gateway. The NIDP system is deployed to detect and report any intrusion attempt to network administrator. It performs its function by carrying out deep data flow inspection after the firewalls. Various kinds of NIDP systems are available in the literature such as Snort, Dragon, RealSecure, etc. in which Snort is a tool of choice in this study due to its features that will be discussed in detail in the next chapter. One of the features that make it attractive is its lightweight rules description language, which is very flexible and powerful. Snort enables users to write their own rules that can be used as a policy to filter the network traffic.

To mitigate invisible attacks, the rule shown in Figure 4.4 is created, designed and tested using Snort, and is stored in its database to be further utilized as a policy.

```
Alert tcp any any -> $HOME_NET any (content:"Filetype"; msg: "Our Organization is infected
with a risk of invisible attack"; threshold: type limit, track by_src, count 1, seconds 120;
classtype: policy-violation; sid: 7000002;)
```

Figure 4.4: Snort rule.

As shown in Figure 4.4, the particular NIDP system rule can be divided into two parts: 1) rule header, and 2) rule options. The text up to the first parenthesis written in blue colour represents the rule header. The section enclosed in parenthesis is the rule options, and the words before the colons in the rule options section are termed as option keywords. The rule header basically defines the packet's "who", "where" and "what", and also gives the detail about the response. The rule's action, protocol, source /destination IP

address and source /destination ports are certain fields that should be included in the rule header. The rule action, which is the first field in the rule header, guides the NIDP system what to do when it finds a packet that matches the rule criteria. By default, there are five actions available in the selected NIDP system; each action defines the certain behaviour, as follows.

Alert~ generates an alert and then logs the packet

Log~ logs the packet

Pass~ ignores the packet

Activate~ alerts and activates the dynamic rule

Dynamic~ remains idle until activated by an activate rule, then acts as a log rule

In this scenario, the executed action is “Alert” as it is very important from security point of view that network administrator should be notified immediately for immediate action. The next field defined in the rule header is protocol and currently, the selected NIDP system is capable to analyse traffic for TCP, UDP and ICMP protocols for suspicious characteristics. In the created rule, TCP protocol is employed.

There is no need to specify source/destination IP and source/destination port numbers because this rule is responsible to inspect traffic coming in from or going to any machine. The Alert messages and packet sections to be inspected are described in the rule options, which contain contents that the packet information should match for the packet to be flagged as malicious. In our case, if a packet contains certain Google dork operators such as filetype,

allintext and allintitle etc. in message contents, then NIDP system will alert the administrator by a generating a message composed in the next field of rule options section. The other fields in the rule option section are thresholds, which specify interval alerts. In the created rule, threshold with type limit is used to generate alert after every 2 minutes.

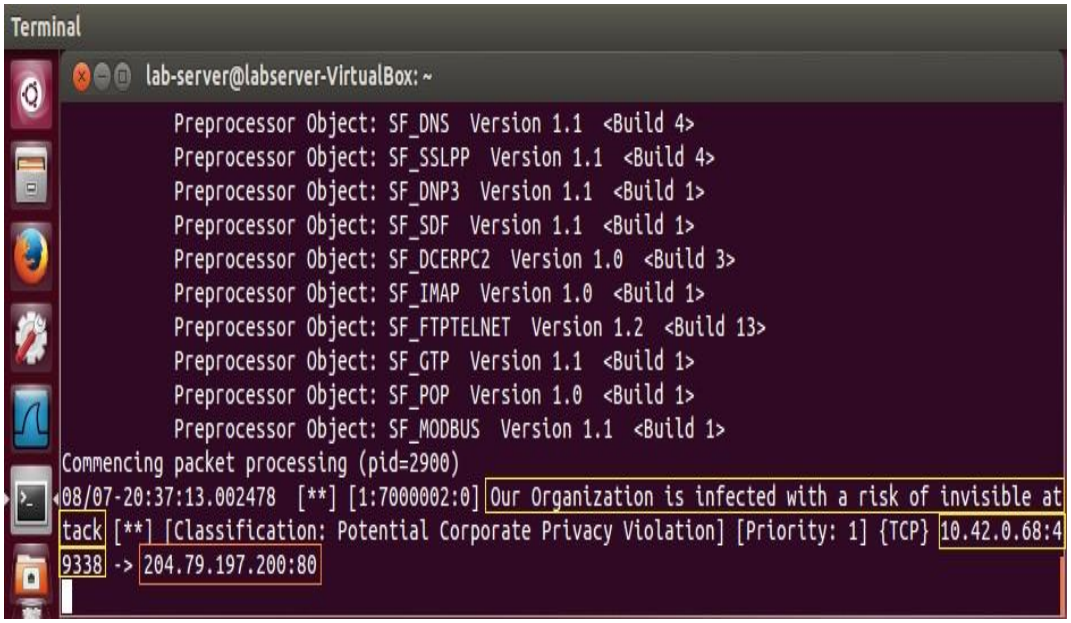

Figure 4.5: The alert received when a test case is performed by trying to query using Google dork operators on the network.

After adding the created rule in NIDP system rules database to evaluate the company network against invisible attacks, the specific commands are generated, which are detected by the company NIDP system as shown in Figure 4.5. The results achieved in Scenario-1 show that, by creating a rule in the NIDP system, a network can be secured against invisible attacks.

4.3.2.2 Scenario II

It is crucial to ascertain the risks and points of vulnerability in computer systems. However, it is also important to estimate the risk quantitatively

associated with the company network. For this purpose, OWASP risk rating methodology is employed to assess the security risk level of company Sales department against invisible attacks. The reason for selecting OWASP tool is its simplicity and capability to address the challenges faced by web application security in a better way. Due to its features, it is widely used by designers, developers, code reviewers, and the quality assurance team.

In this scenario, the attacker gets advantages of company's invisible vulnerabilities (usernames and passwords) by generating invisible attacks using Google advanced search engine and retrieves company's confidential information. The standard risk model is particularly involved into 4 steps, described as follows.

- Step-I: Identification of risk

In risk assessment, the first and foremost step is the identification that needs to be rated. For this purpose, a network administrator collects information regarding threat agents, vulnerabilities, attacks and their impacts on organization. In our specific case, the threat agents are particularly competitors interested in stealing company's Sales information. Usernames and passwords are the vulnerabilities that can be exploited by threat agents to achieve their targets, whereas, Google dorks are the threats.

- Step-II: Factors for estimating likelihood

Factors involved in estimating likelihood are further classified into two categories: 1) Threat agent factors, and 2) Vulnerability factors. Let A(L) represents the option in the likelihood factors, where "A" shows the particular attribute and "L" describes its level.

1. Threat agent factors

The term threat agent can be used to specify a single attacker or a group of attackers that actually generates attacks. The factors involved in the context of threat agents to estimate the probability of a successful attack are skill level, motivation level, opportunity and size of the threat agent.

- Skill level

Skill level specifies the attacker's capability to exploit the weaknesses of the system. Different options listed for threat agent's skills are given below.

× No technical skills (1)

✓ Some technical skills (3)

× Advanced computer user (4)

× Network and programming skills (6)

× Security penetration skills (9)

In this particular scenario, "Some technical skills" is a better option to focus on because it does not require any penetration, programming or advanced skill to retrieve vulnerability of the network.

- Motive

Motive refers to the level of interest of threat agents exploiting the weaknesses of the network system.

× Low or no reward (1)

✓ Possible reward (4)

× High reward (9)

It is a good option to select “Possible reward (4)” because normally threat agents make query about company information during exploration. This is an information gathering stage and the recorded information is then used for estimating the value associated with the possible attack on the company. Since, the company under consideration was not secure; therefore, the gathered information could be utilized to access systems having company financial data and its resources.

- Opportunity

Opportunity outlines the resources required for attacker to manipulate and exploit the vulnerable components of the network.

× Full access or expensive resources required (0)

× Special access or resources required (4)

✓ Some access or resources required (7)

× No access or resources required (9)

“Some access or resources required (7)” is a good choice to select from the given choices since the threat agent only needs to evaluate the invisible attacks by exploiting time, Internet and proper Google dork commands.

- Population size

The population size refers to the number of people involved in generating the attack as well as exploiting the vulnerability of the system.

× Systems administrators (2)

× Intranet users (4)

× Partners (5)

× Authenticated users (6)

✓ Anonymous Internet users (9)

“Anonymous Internet user (9)” is a better option to focus on because severity risk assessment is associated to the Internet especially from outside the network. Note that the remaining options are for the legitimate users of the organization.

2. Vulnerability Factors

The purpose of this factor is to predict the likelihood of discovering and exploiting specific system vulnerabilities. It is assumed that the attacker has sufficient knowledge to use Google dork operators and knows how to create a command from these operators in order to query specific vulnerabilities. The factors that affect the discovery and exploitation of system vulnerability are given below.

- Ease of discovery

Different vulnerabilities have different discovery levels depending upon the attacker’s skill and the tools necessary to create potions. Following are the various options used to determine how easy to discover a vulnerability.

× Not applicable (0)

× Practically impossible (1)

× Difficult (3)

✓ Easy (7)

× Automated tools available (9)

It is good to select option “Easy (7)” because it is easy to discover vulnerability by Google dork operators and there is no need to use any other tool or sophisticated skills.

- Ease of Exploit

Having discovered the vulnerability, there is a need to measure how easy to utilize it in order to compromise the system.

× Not applicable (0)

× Theoretical (1)

× Difficult (3)

✓ Easy (5)

× Automated tools available (9)

Since the information discovered during the experiment is very sensitive and can be utilized by threat agents to gain access to different company network resources easily, therefore, “Easy (5)” is a good option to select from the given options.

- Awareness

This factor describes how much familiar the attacker is with the vulnerability.

× Not applicable (0)

× Unknown (1)

- ✓ Hidden (4)
- × Obvious (6)
- × Public knowledge (9)

The option “Hidden (4)” is selected because vulnerability discovered through Google dorks is an invisible form of attack, i.e. the vulnerability is hidden to the attacker.

- Intrusion detection

This factor measures intrusion due to exploitation of vulnerability by the system security countermeasures.

- × Not applicable (0)
- × Active detection in application (1)
- × Logged and reviewed (3)
- ✓ Logged without review (8)
- × Not logged (9)

The system security countermeasures log the query as it is viewed as normal traffic. The logs are not marked for review, which implies that no intrusion will be detected. Since the information discovered is legitimate, therefore, the invisible attack is seen as normal traffic.

Now, all these options selected from Threat Agent Factors and Vulnerability Factors are summarized in Table 4.3.

Table 4.3: Likelihood Factors.

Threat Agent Factors	
Skills required	Some technical skills (3)
Motive	Possible reward (4)
Opportunity	Some access or resources required (7)
Population size	Anonymous Internet users (9)
Vulnerability Factors	
Easy of discovery	Easy (7)
Ease of exploit	Easy (5)
Awareness	Hidden (4)
Intrusion detection	Logged without review (8)

- Step-III: Factors for estimating Impact

When vulnerabilities are exploited, the company network as well as its resources is compromised. This affect can range from low level to the high level, for example shutting down the business. There is a need to measure the impact of attack on the company network. This impact can either be on the technical level or on the whole business. Now, we discuss and measure these factors based on the case study. Assume that $\mathrm{A(L)}$ is the option in the impact factors, where “A” shows the particular attribute and “L” describes its level.

1. Technical Impact Factors

This impact factor describes the effects of attack on the company network and its resources. Based on the security properties, these impact factors are classified into confidentiality, integrity, availability and accountability.

- Loss of confidentiality

The term loss of confidentiality assesses the amount of data that can possibly be disclosed by invisible vulnerability.

× Not applicable (0)

× Minimal non-sensitive data disclosed (2)

× Extensive non-sensitive data disclosed (6)

✓ Extensive critical data disclosed (7)

× All data disclosed (9)

The data disclosed in the case study contains sensitive information such as usernames and passwords that can be used to access both the company network and data systems.

- Loss of integrity

The loss of integrity refers to assess the amount of data that can possibly be corrupted or damaged in case of a successful attack.

× Not applicable (0)

× Minimal slightly corrupt data (1)

× Minimal seriously corrupt data (3)

× Extensive slightly corrupt data (5)

× Extensive seriously corrupt data (7)

✓ All data totally corrupt (9)

During analysis, it was found that the retrieved information contained logins with high privileges, which could be used to access any network resource in the Sales department as well as could be altered leading to corrupting entire department data. Since the financial software used in the Sales department has a chain reaction, i.e. a change in one instance can lead to the change in another instance; therefore, all the other systems in the department can be affected.

- Loss of availability

Loss of availability assesses how the exploitation of vulnerability can impact the network services availability. In this regard, the following question can arise:

- Will the attack lead to the network down?
- Will there be any disruption in service due the attack and how critical will be the impact of services on the functionality of the network?

To answer the above-mentioned questions, one of the following options can help to quantify the impact of loss of availability on network.

✓ Not applicable (0)

× Minimal secondary services interrupted (1)

× Minimal primary services interrupted (5)

× Extensive secondary services interrupted (7)

× All services completely lost (9)

Since the information retrieved is from the Sales department, therefore, accessed login details will pose no effect on the network services. However, it is worth mentioning that this information can be used as a stepping stone to gain more access to the network in order to disrupt network services.

- Loss of accountability

Once the attack is successful, this factor helps in quantifying how security countermeasures can be used efficiently to track the changes and also trace them back to the point of exploitation.

× Attack fully traceable to individual (1)

✓ Attack possible traceable to individual (7)

× Attack completely anonymous (9)

It is better choice to select “attack possible traceable to individual (7)” because security countermeasures can trace the changes of user login used by the attacker. Since, the information like user logins and passwords has already been disclosed by the attacker, so the legitimate user will not be accountable for the misuse of the account. However, it is possible to trace the account but it is difficult to trace the individual generated the attack.

2. Business Impact Factors

The business impact comes from technical impact requiring a good understanding of what is important to the company from application point of view. These impact factors are the common areas for various organizations

and these areas are particularly more unique to a company than the factors associated with threat agent, vulnerability, and technical impact. Some details of each of these factors along with their respective options are given below.

- Financial damage

This factor measures the financial impact of the attack. This can cause decrement in annual profit, loss of major accounts, and in some cases the organization can become bankrupt.

× Not applicable (0)

× Damage cost less than to fix the issue (1)

× Minor effect on annual profit (3)

× Significant effect on annual profit (7)

✓ Bankruptcy (9)

Using worst case scenario, the attacker is assumed to have access to financial reports and financial systems, then, it will be easy for the attacker to mislead the Sales department and thus making the business bankrupted.

- Reputation damage

This factor affects the company name and its stakeholders. It also causes loss of major clients as well as goodwill.

× Not applicable (0)

× Minimal damage (1),

× Loss of major accounts (4)

× Loss of goodwill (5)

✓ Brand damage (9)

The selected option is “brand damage (9)”, because once the company has been declared a compromised; it will be difficult for it to attain the client trust again.

- Non-compliance

How much exposure does non-compliance introduce?

× Not applicable (0)

× Minor violation (2)

× Clear violation (5)

✓ High profile violation (7)

High profile violation is a better choice to select for this scenario.

- Privacy violation

This factor has a number of effects, for example, loss of sensitive personal information may result in identity protection violation. The loss of commercially sensitive information may lead to legal liabilities.

× Not applicable (0)

× One individual (3)

✓ Hundreds of people (5)

× Thousands of people (7)

× Millions of people (9)

Since, the company under consideration is a small enterprise so the information disclosed is of hundreds of people. Bigger companies will have bigger exposure.

Now, all these selected options from Technical Impact Factors and Business Impact Factors are summarized in Table 4.4.

Table 4.4: Impact Factors.

Technical Impact Factors	
Loss of confidentiality	Extensive critical data disclosed (7)
Loss of Integrity	All data totally corrupt (9)
Loss of Availability	Not applicable (0)
Loss of Accountability	Attack possible traceable to individual (7)
Business Impact Factors	
Financial damage	Bankruptcy (9)
Reputation damage	Brand damage (9)
Non-compliance	High profile violation (7)
Privacy violation	Hundreds of people (5)

➢ Step-IV: Determining the severity of the risk

The level from 0 to 9 is further divided into three sublevels: 0-3, 3-6 and 6-9 representing low, medium and high level respectively as given in Table 4.5.

The overall severity risk level is calculated based on the likelihood and impact estimates using the security risk assessment Table 4.6. These risk levels may be low, medium, high or critical.

Table 4.5: Likelihood and Impact levels.

[0, 3)	Low
[3, 6)	Medium
[6, 9)	High

Table 4.6; Overall severity risk level of invisible attack.

	Impacts		
Likelihood	Low	Medium	High
Low	Note	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

Finally, the overall risk severity level of the invisible attack on Sales department is calculated as follows. Let n_L and n_I represent the total number of options, selected from likelihood and impact factors respectively, $A_L(L)$ and $A_I(L)$ denote the respective level values of the particular options being selected as better choices from likelihood and impact factors. LS and IS represent the likelihood and impact scores respectively, are defined as:

$$LS = \frac{1}{n_L} \sum_{Level} A_L(L) \quad (4.1)$$

$$IS = \frac{1}{n_I} \sum_{Level} A_I(L) \quad (4.2)$$

Using Table 4.3 and Table 4.4, after plugging the values in equations (4.1) and (4.2), we come up with:

$$LS = \frac{1}{8}(3 + 4 + 7 + 9 + 7 + 5 + 4 + 8) = 5.87 \quad (4.3)$$

$$IS = \frac{1}{8}(7 + 9 + 0 + 7 + 9 + 9 + 7 + 5) = 6.62 \quad (4.4)$$

Since, $LS \in [3, 6)$ and $IS \in [6, 9)$, which implies that likelihood score has a medium risk severity level, whereas, impact score possesses a high risk severity level. Now, using security risk assessment Table 4.6, the corresponding risk severity level for $\{(\text{medium}, \text{high}),\ \text{medium} \in \text{likelihood} \text{and} \text{high} \in \text{impact}\}$ is high. Therefore, in the light of the above analysis, it can be concluded that the overall risk severity level on Sales department of UK based company caused by invisible attack is high.

4.4 Conclusion

The overview of different types of attacks with respect to their visibility to security countermeasures has been discussed and concept of invisible attacks based on literature and experimental studies was elaborated in this chapter. The Google dorks as the invisible attacks were tested by

considering a UK based company as a case study. The results of this study will be helpful in these ways:

- To design methods for countermeasures against security attacks and mitigation purpose.
- To define the priority attached to the rule written in the NIDP systems based on the impact of the attack.

These two contributions can help the network management team to build more secure networks especially against the invisible attack.

Chapter 5.

NIDS RISK ASSESSMENT

5.1 Introduction

There is increasing concern amongst computer security communities about the rising number of malicious attacks. Firewalls and intrusion detection systems (IDS) are the main components widely used to counter security threats. Implementing firewalls in a network is considered a major deterrent to network threats. Despite the protective mechanism, a firewall does not provide full protection against data leakage and, hidden and multithread attacks. However, to be protected from these attacks and to have a more secure network against unwanted malicious traffic, sophisticated intrusion detection/prevention tools are required. The tools termed as IDS analyze the traffic in depth and decide whether the traffic is normal (friendly) or malicious (hostile). If the traffic is hostile, the system generates alerts. The IDS have been proved quite effective and with the increasing number of threats, majority of network communities have been investigating how to produce a more effective network intrusion detection and prevention (NIDP) system.

The main problem with the current NIDP systems is that they lose packets in case of high traffic volumes. This affects the assessment of risk security levels of the organization. Therefore, packet loss is one of the significant problems faced by the networking teams today. To increase the security of a network, there is a need to evaluate the performance of existing NIDP

systems. Assessing the security risk level of malicious traffic running in a network is also another major problem which needs a special attention. Currently deployed NIDP systems show the qualitative risk level of attacks in terms of high, medium, low and very low. These fuzzy measures are not enough to describe the security risk level of a network. There must be a quantitative metrics which shows the security risk level produced by attacks based on absolute value.

This chapter is divided into two scenarios. Scenario-1 employs the performance evaluation comparisons in terms of packet handling capability of two NIDS tools, Snort and Suricata under three different platforms (Linux, FreeBSD and ESXi server). The proposed and designed methodology is performed on a specifically designed test bench to replicate busy enterprise network traffic. Scenario-2 describes how the security risk level of attacks in the presence of NIDP system is assessed. The following experiments will help network administrators to:

- Choose the most suitable NIDP system for their network in terms of packet handling capability;
- Quantitatively assess the security risk level of a network by creating NIDS security metric based on best traffic speed used for analysing network traffic.

5.2 Snort Overview

Snort is a well-known name in the information security community. It was developed by Martin Roesch in 1998 [84]. It is an open source NIDP system

that combines the benefits of signature, protocol, and anomaly based inspection to detect hostile traffic. It is capable of performing packet logging and real-time traffic analysis on the network [85]. Snort inspects packet header and performs protocol analysis. It monitors a range of network threats by using content/signature matching algorithms and logs the traffic on the network, and generates alerts against malicious events [86], [87]. The main function of Snort and other types of NIDP systems is to effectively analyse all the traffic passing through the network without any packet drops. Its architecture is usually composed of four components: packet sniffing, pre-processor, detection engine and output device as shown in Figure 5.1.

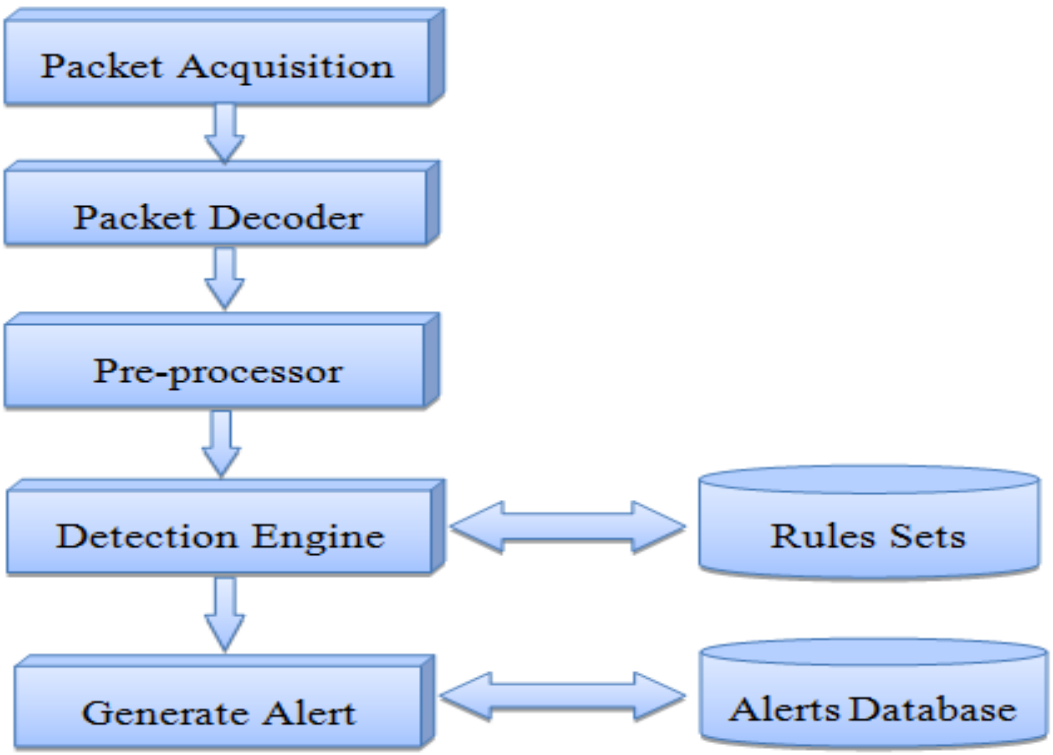

Figure 5.1: Snort Architecture.

In case of packet sniffing, Snort collects data from the network and displays it as it is on the screen in a TCP dump mode. It relies on libpcap and winpcap

libraries for packet acquisition, where Libpcap and winpcap are specific platforms used to receive traffic from the network. Packet acquisition monitors packet arriving time and calculates total length of the packet, and also checks interface link type on which the packet was captured. Snort processes single packet at a time and if there is a vast volume of traffic on the network, it takes a little longer to handle that traffic. The buffering system is a major limitation in Snort as it drops excess packets causing some of the packets to bypass the detection engine which leads to compromising the network. The second step of packet processing is packet decoding, in which decoders examine the link layer and try to find out the layer used for packet fetching. Snort can be configured by different links such as Token, Ring, Bus, FDDI, Cisco, SLIP and Point to Point, etc. With the help of pcap files, Snort analyses the traffic on each link layer and if it finds any malicious packet, it begins to make a queue for that traffic. Packet decoding in Snort is straightforward especially for an Ethernet link. At TCP packet decoding, Snort makes the structure of packets and sends them towards the protocol decoder [88]. After decoding, it forwards these packets towards pre-processor for performing various operations like examining protocols and their behaviour for anomaly-based detection. All the information going to pre-processor must pass through the protocol decoder. The main pre-processors in Snort are packet defragmentation, Stateful inspection session and application layer. A pre-processor is basically a program used to normalize the raw packets and checks them against anomaly-based behaviour, for example HTTP plug-in manages the application at traffic flow time and also avoids unwanted traffic processing that can cause an overload on the

network. The output of Snort pre-processor becomes the input of the detection engine. Some of the basic functions of the pre-processors are protocol normalization, anomaly-based detection (non-rule based detection) and statistics-based detection. In case of TCP, the pre-processor divides data into smaller frames of datagram and sends them to the destination by labelling them with unique identifiers [88]. On the destination, all these fragmented datagrams are reassembled. If any of the sequence numbers in a datagram reassembling is missing, TCP again sends the datagram frame to the destination until it receives a positive acknowledgement from the destination. In the case of UDP, there is no retransmission because the destination does not send any acknowledgement.

Detection engine is one of the key components of Snort which works differently to the pre-processor. Its basic purpose is to get data or packets from the pre-processor and matches the pattern of the received packet with the database of a certain set of rules. If pattern matches then it generates alerts against the malicious packet and stops working on that specific packet. Otherwise, Snort treats the packet as a normal traffic and does not generate any alert against it. The detection engine generates alerts or logs depending upon the rule, for example, if the rule is of low priority then there will be a low level alert. In NIDP system mode, the higher the traffic volume that Snort has to handle, the higher the number of packets drop.

5.3 Overview Suricata

Like Snort, Suricata is an open information security foundation (OISF) funded by the USA Department of Homeland Security's Directorate for Science and

Technology (HOST) program and the Navy's Space and Naval Warfare System Command Open Security Technology program [89]. It is also a rule based NIDP system that takes advantage of externally developed rule sets to monitor network traffic and provide alerts when suspicious events take place [27]. Like most IDSs, it is designed to fit within existing network security components. It works as a multithreaded engine and according to its creators, the objective of the Project Phase-1 was to have a distributable and functional NIDP system engine. On 1st January 2010, it was first made available for downloading for academic and non-commercial research purposes [89]. Its structure is written in C language and supports FreeBSD, Linux, UNIX, Mac OS platform. The source code for configuration file is written as a YAML file. In comparison with Snort, Suricata can process from one packet to tens of thousands/hundreds of thousands packets at a time. There is a trade-off between lower performance and less memory (RAM) or higher performance and more memory. In other words, memory usage increases, the performance decreases when Suricata processes huge number of packets [89].

After acquisitioning a packet, like Snort, Suricata decodes it and then forwards it to the pre-processor as shown in Figure 5.2. Since the packets received on a network are fragmented, therefore, defragmentation is applied to the packets before going to Suricata for further inspection. The defragmentation session contains prealloc, timeout and max-frag options. To save system resources, signatures are divided into four different categories:

default, high, medium and low. The detection engine is designed to provide the best balance of performance and memory usage.

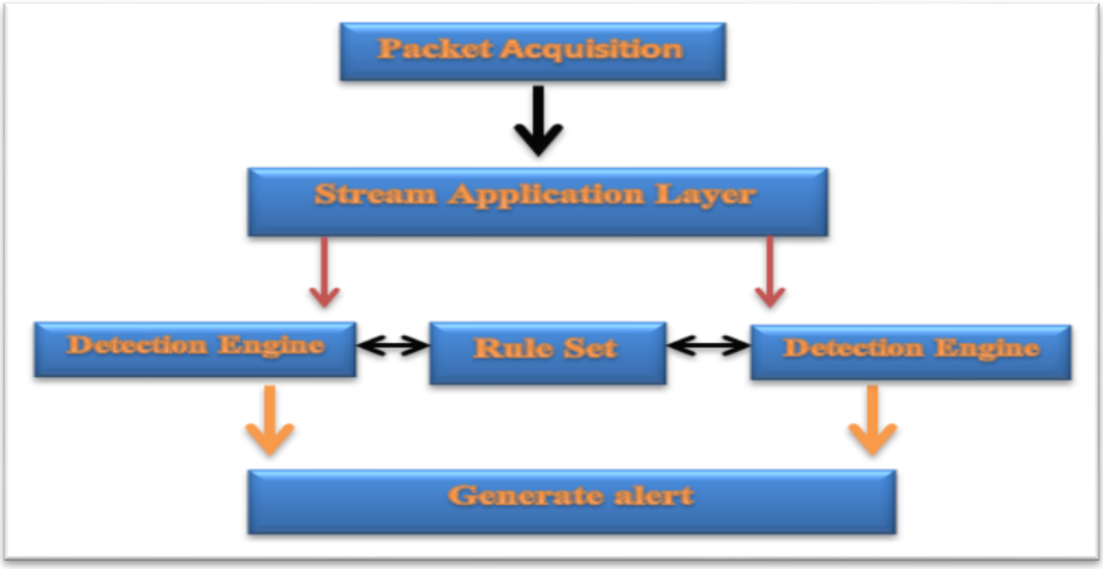

Figure 5.2: Suricata architecture.

5.4 Test Bench

The tests have been performed on a real network composed of high performance PCs used to generate desired traffic. The NIDP systems running Snort/Suricata and a ProCurve series 2900 switch is shown in Figure 5.3. The PCs are connected via the switch using a 1.0 Gigabit cables and two 10 Gigabit cables. The port connecting the NIDP system to the network on the switch acts as a spanning port. Fixed numbers of packets are generated from source to destination for both NIDP systems. The packet size representing the amount of data is defined in the packet. The maximum data size for TCP and UDP connections is 65536 bytes and 65507 bytes respectively. The LAN traffic V2 enhanced tool is taken into account for generating traffic from source machines to destination machines.

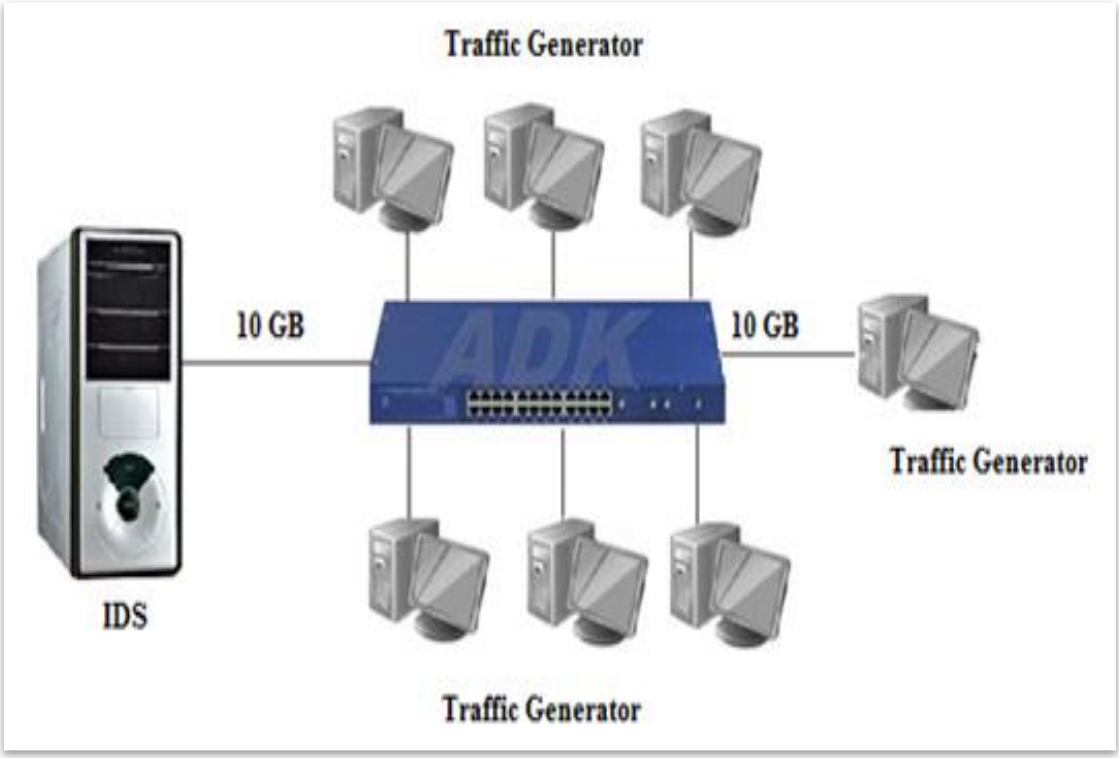

Figure 5.3: Test bench.

The NIDP systems used in this experiment are signature based IDSs containing built-in rules. It is important to note that the best IDS is not the one having the most rules (signatures) but the one that performs better in detecting attacks and avoids false positives irrespective of its internal architecture or behaviour. More rules mean additional chances to catch malicious traffic. The same numbers of rules, i.e. 8000 are loaded in the databases of both NIDP systems (Snort and Suricata) in all experiments.

Now, in this experiment the main focus is the number of packets received, analysed and dropped by the NIDP systems. The readings are taken from the summary of NIDP systems after running for 1 minute, 5 minutes and 10 minutes. The application's usage (CPU usage) is calculated from the system

task manager. The hardware specification of the network components is shown in Table 5.1.

Table 5.1: Network components specifications.

Machine Type	**Hardware Specifications**	**Tools used**
Windows SP2	Dell Precision, T3400,Intel Quad-core,Q6600,2GB Ram, 1Gbps network card	LAN Traffic Generator
FreeBSD Linux 2.6	Dell Precision, T3400,Intel Quad-core, Q6600,2GB Ram ,10Gbps network card	Suricata, Snort Bandwidth monitor
ESXi Server	Dell Precision, T3400,Intel Quad-core, Q6600,4GB Ram, 1Gbps network card (for monitoring server), 10Gb for IDS	VMware ESXi Hypervisor Linux 2.6 Suricata, Snort Bandwidth monitor
Attacker	Dell Precision, T3400,Intel Quad-core, Q6600,2GB Ram , 1Gbps network card	Backtrack Linux Metasploit 3 Framework
Network Switch	ProCurve series 2900	

5.4.1 Scenario-1

Test scenarios-1 is designed to compare the performance of Suricata with Snort on different operating systems for different tasks. Both NIDP systems are subjected to the same tests under the same operating conditions. To attain more accuracy in results, all tasks are performed on packet sizes 512 bytes, 1024 bytes and 1470 bytes for the different protocols with speeds 250 Mbps, 500 Mbps, 750 Mbps, 1.0 Gpbs, 1.5 Gbps, and 2.0 Gbps. Both NIDP systems are configured to load and run a similar number of rules to monitor the traffic generated. The assessment of more reliable IDS on a busy network is achieved on the basis of number of packet drops. The following tasks will provide a clear view of the test scenario-1.

Task A: Performance of NIDP systems on ESXi sever

Most data centres use virtualization as a means of saving time and money. This is a common practice in the enterprise environment. To ensure the validity and accuracy of the experiments, both NIDP systems are operated in exactly the same environment and, to simulate an enterprise's data centre, both tools are implemented on ESXi server [90]. Since, this is a performance assessment; the machines should be as identical as possible in terms of hardware to enable an accurate comparison. The ESXi server is equipped with 4GB RAM in which 2GB is allocated to the virtual Linux running inside the ESXi server. A network card is employed in the ESXi server to establish a connection from the management PC to the virtual host.

Task B: Performance of NIDP systems on Linux 2.6

In this task, Snort and Suricata are operated on a Linux 2.6 server running Ubuntu 10.10. The machine is configured to monitor traffic using 10 Gbps card.

Task C: Performance of NIDP systems on FreeBSD

Snort and Suricata are operated on a FreeBSD server running the latest version 8.1, which is configured to operate with 10 Gbps network card. Both NIDP systems are operated separately on the same platforms allowing them to use all the available resources.

5.4.1.1 Result and Analysis

This section covers the results and analysis of the performance evaluation for both Snort and Suricata on the three different platforms. For clarity and understanding, this section is further divided into two subsections: TCP and UDP traffic. Each subsection delivers a performance comparison on a virtual machine, Linux 2.6 and FreeBSD with different packet sizes and speeds.

- TCP

Figure 5.4 illustrates the performance of both NIDP tools using packet size 512 bytes. In this test, Suricata shows some packet drops in the early stages (250 Mbps), but on Virtual Linux, it reaches 35.4%, which is considered as high packet drops at a low traffic speed. It is also observed that Suricata has some small packet drops of 0.6% on FreeBSD and no packet drops on Linux 2.6. This percentage of packet drops increases slightly when the speed goes to 500 Mbps. As shown in Figure 5.4, Snort performs very well as there are no packet drops recorded at 250 Mbps and 500 Mbps on all platforms. Once

the speed approaches to 750 Mbps, Snort drops 1.1% of the packets but it does not drop any packets for Linux 2.6 or FreeBSD system setup.

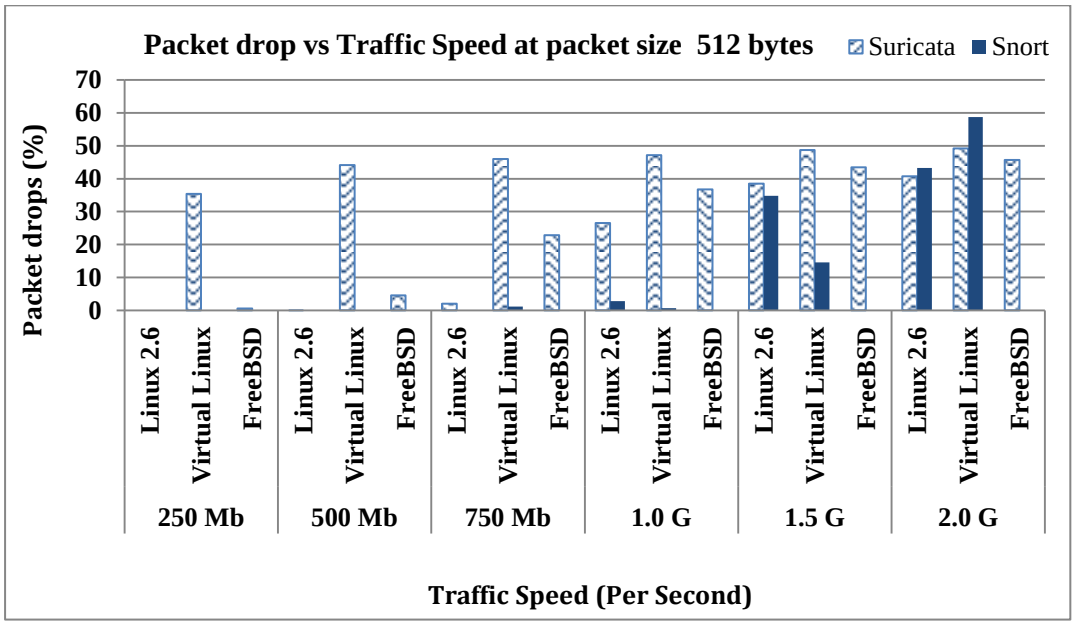

Figure 5.4: Comparison chart of Snort and Suricata (512) TCP.

At 1.0 Gbps, Suricata continues to drop packets (26.5% on Linux 2.6, 36.7% on FreeBSD and 47.2% on virtual Linux) while Snort performs better with only 2.8% and 0.6% packet drops for Linux 2.6 and virtual Linux respectively. At high speeds, Snort does not behave well with packets drops of upto 60% on Virtual Linux while Suricata gains ground with lower packet drops than Snort. From the results, it is clear that although the speed affects the number of packet drops for Snort, Suricata tends to consistently drop packets no matter the traffic speed.

At packet size of 1024 bytes, the results compiled from the experiment are shown in Figure 5.5. Similar to the results achieved in the earlier test, Suricata drops packets for all traffic speeds when using the Virtual Linux platform and also shows low percentage packet drops for the other platforms

until the speed hits 750 Mbps. Snort, on the other hand exhibits good performance for the low speeds but drops a high percentage of packets (27.8%) at 1.5Gbps.

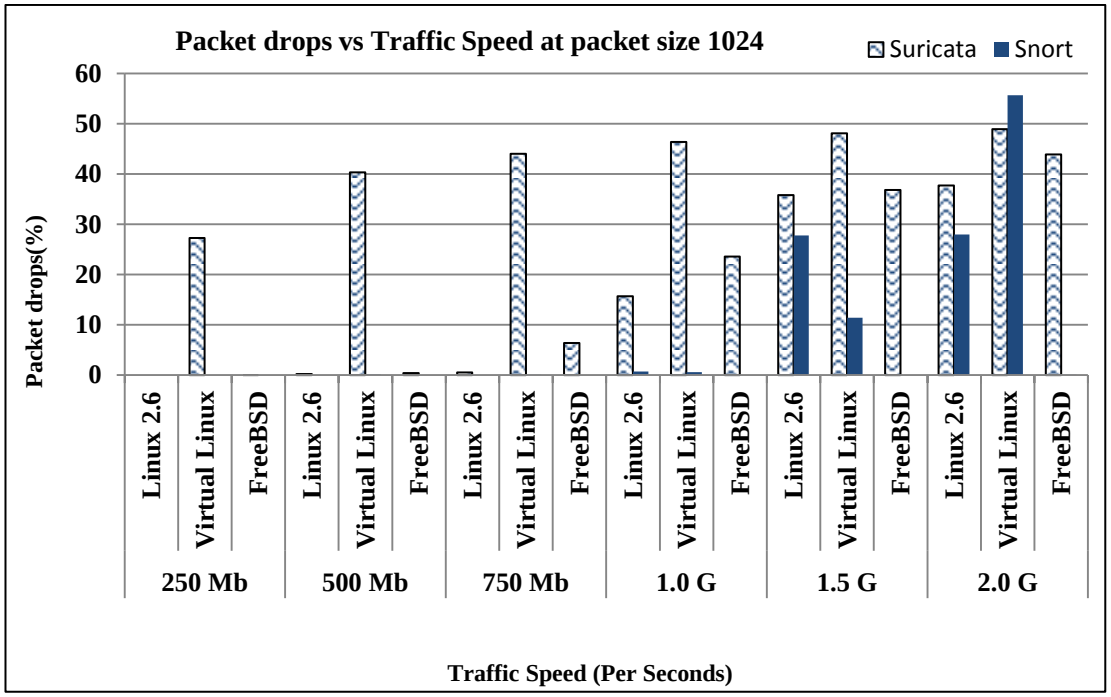

Figure 5.5: Comparison chart of Snort and Suricata (1024) TCP.

It is worth mentioning that the performance of Suricata on Linux2.6 at the speed of 750 Mbps is improved as the number of packet losses does not exceed 0.5% on Linux 2.6 and 6.4% on FreeBSD. Suricata records a high jump in the number of packet drops at 1.0 Gbps as it reaches 15.7% on Linux 2.6, 23% on FreeBSD and 46% on Virtual Linux. On the other hand, Snort only drops 0.7% on Linux 2.6, 0.56% on Virtual Linux and 0% on FreeBSD. Once the traffic speed approaches to 1.5 Gbps, there is a significant increase in the packet drops on Linux 2.6 as well as virtual Linux up to 27.8%. Suricata at this stage records 35% on Linux 2.6 and more than 48% on Virtual Linux, whereas, Snort records only 11%. At 2.0 Gbps, there is

a clear difference in Snort's performance on Virtual Linux as it drops more than 55% packets while the packet drop is only 11% at 1.5 Gbps. This shows that the platform used by the NIDP systems also determines its performance.

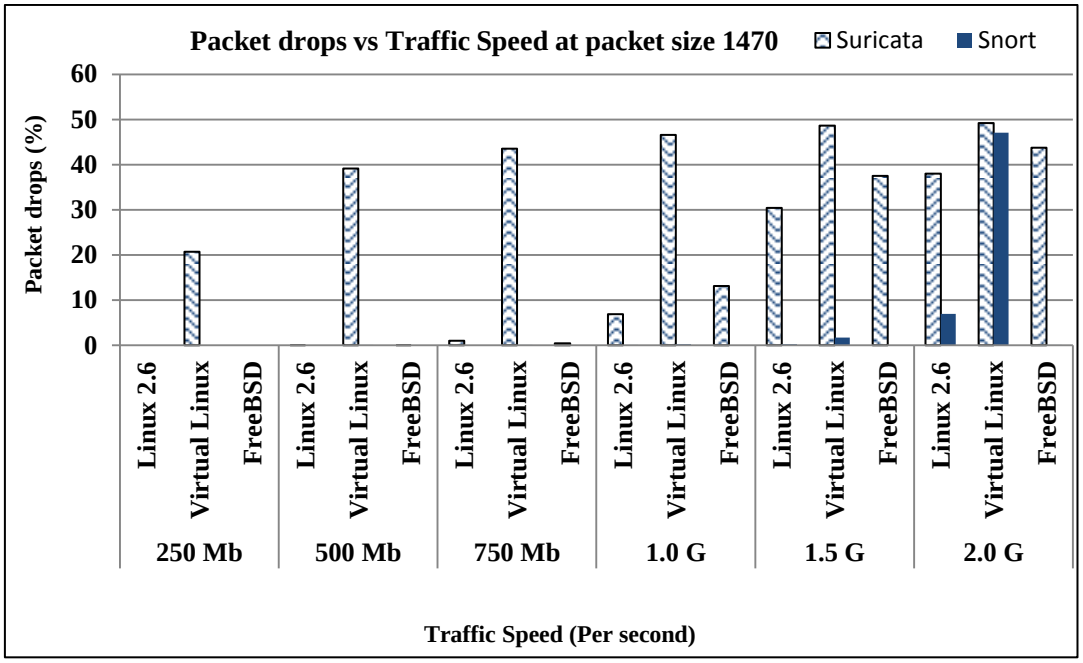

Figure 5.6: Comparison chart of Snort and Suricata (1470) TCP.

Figure 5.6 shows the performance of both systems when dealing with a larger packet size (1470 bytes). The performance in this test is quite similar to the previous one. Suricata performs the same way with high packet drops observed when running in the Virtual Linux environment across all speeds, whereas, at the other platforms, it first exhibits the packet drops at 1.0 Gbps (6.86% and 13.1%), and this percentage of packet drops increases with increasing the speeds. Snort on the other hand, does not drop packets at all the platforms until the speed of 1.5 Gbps (1.68%). By analysing all three experiments carried out for the TCP packet sizes, it is clear that Snort shows a more predictable performance rate than Suricata.

➢ UDP

Suricata records some packet drops at a low speed (250 Mbps) as shown in Figure 5.7. This packet drops is recorded when dealing with a packet size of 512 bytes. Although, there is a large number of packet drops on virtual Linux and FreeBSD but there is no packet drop recorded on Linux. At this speed, Snort is performing well with no packet drops at all the platforms.

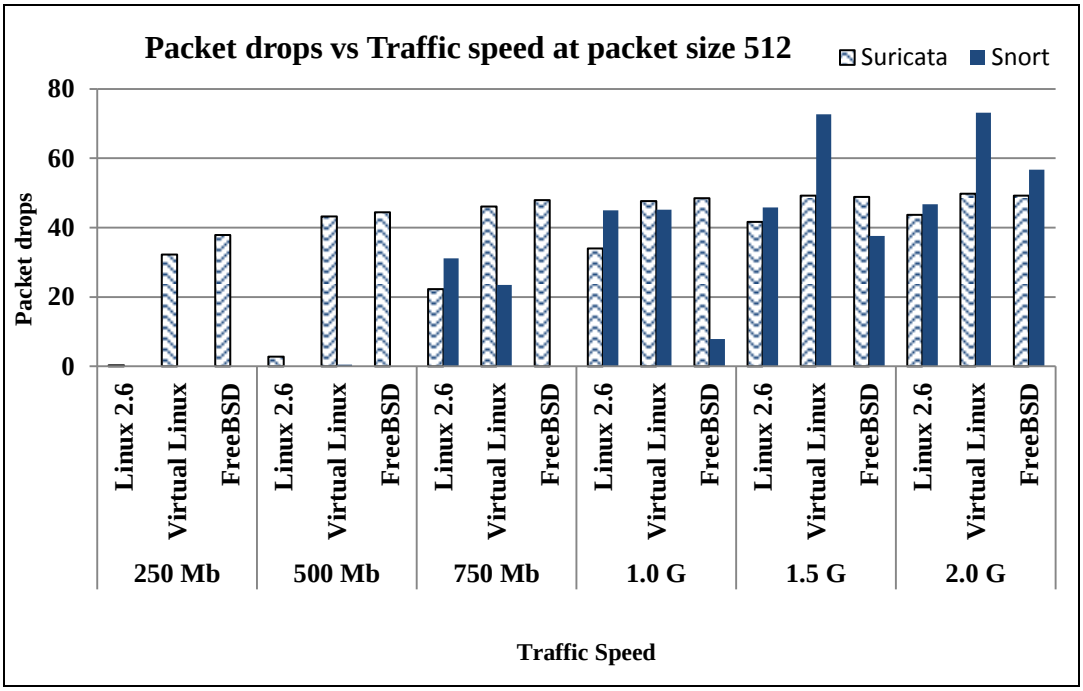

Figure 5.7Comparison chart of Snort and Suricata (512) UDP.

When the generated traffic approaches to speed 500 Mbps, Suricata again shows a high percentage of packet drops on FreeBSD and virtual Linux but there is a minor increase in the number of packet drops on the Linux 2.6 platform. On the other hand, Snort is still performing better than Suricata, as no packet drops are recorded on Linux 2.6 and FreeBSD, and only 0.48% on virtual Linux. As can be seen from Figure 5.7, Snort makes a significant jump in the number of packet drops on Linux 2.6 and virtual Linux when the traffic

approaches to speed 750 Mbps. It is worth pointing out that Snort is proving to perform best on FreeBSD as no packet drops are recorded up to this speed. At 1.0 Gbps, Snort starts showing some packet loss on FreeBSD 7.9%, and Suricata losses 45%. When the generated traffic reaches speed 1.5 Gbps and above, Snort starts to drop a large number of packets exceeding 73%.

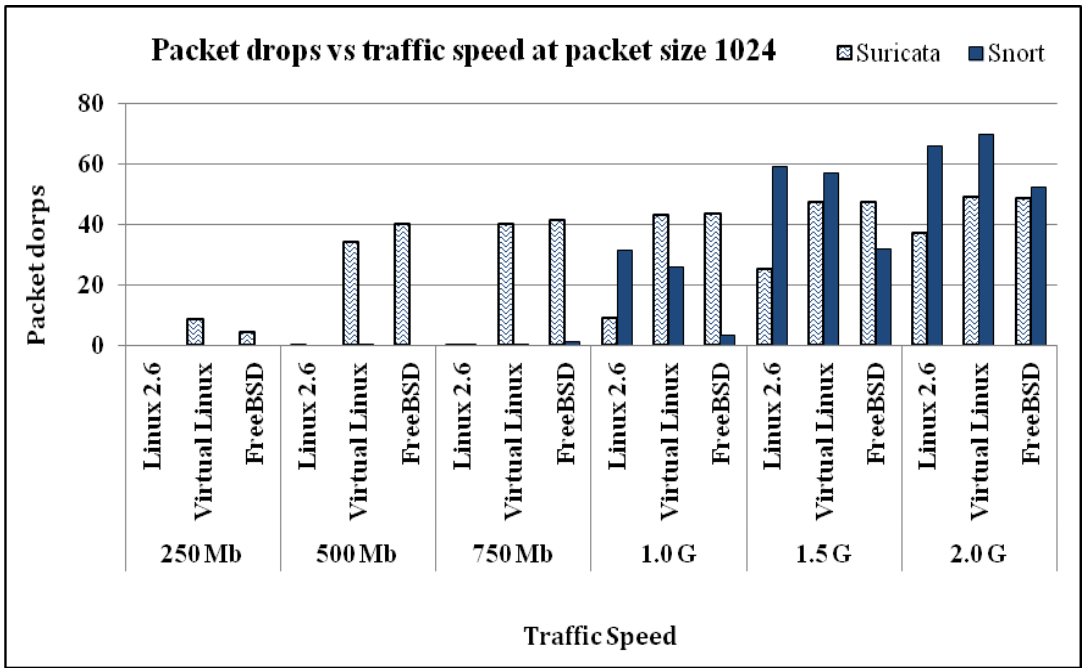

Figure 5.8: Comparison chart of Snort and Suricata (1024) UDP.

At the packet size of 1024 bytes, Snort is still ahead of Suricata in terms of performance as shown in Figure 5.8. Snort does not record any packet losses at the speeds of 250 Mbps and 500 Mbps on Linux 2.6 and FreeBSD, and just 0.1% on virtual Linux. On the other hand, Suricata shows a large number of packet drops as it reaches 40.2% on FreeBSD and 33.9% on virtual Linux. It does not record any packet losses on Linux 2.6 at the same speeds. Suricata's performance at the speeds of 250 Mbps, 500 Mbps and

750 Mbps is acceptable as it does not exceed 0.33%. The overall performance of Snort at the speed 750 Mbps is significantly better on the virtual machine and FreeBSD as it only records 1.2% packet drops. At higher speeds (1.0 Gbps), the best performance is achieved on FreeBSD with only 3.24 % packet drops, whereas the best performance for Suricata is on Linux 2.6 at 8.9%. At the speeds of 1.5 Gbps and 2.0 Gbps, both IDSs drop a large number of packets.

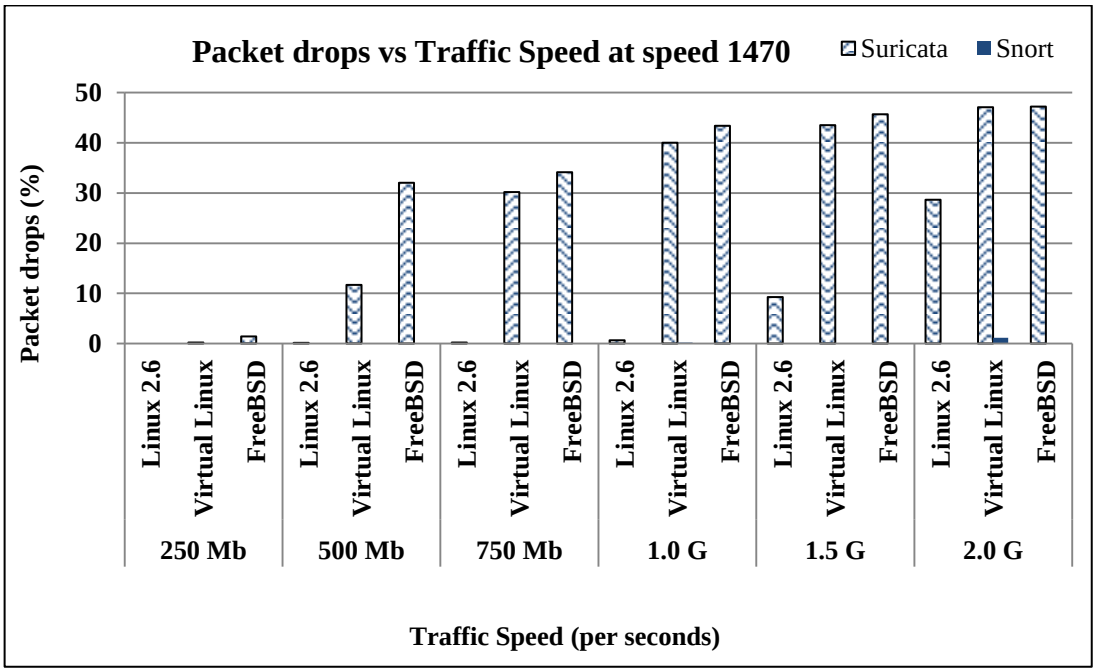

Figure 5.9: Comparison chart of Snort and Suricata (1470) UDP.

Now, from Figure 5.9, Snort percentage of packet drops is noticeable. It can be said that Snort is capable of handling packets of size 1470 bytes effectively than Suricata. Snort starts to drop packets at the high speed of 1.0 Gbps on virtual Linux but does not exceed 1.15% at the speed of 2.0 Gbps.

5.4.1.2 Summary of Analysis

Scenario-1 focused on comparing the effectiveness of the new NIDP systems Suricata with the well-known NIDP system, Snort, in a high speed network environment to determine the best NIDP system. Both NIDP systems were evaluated on different platforms with different protocols and packet sizes. The results show that there is a significant numbers of packet drops when using virtualization, where the allocated physical memory (RAM) of host machine is actually allocated to virtual RAM and disk space [91]. Due to this characteristic, the number of packet received by the network card is higher than the recorded by the virtual machine leading to more packet drops. It is also observed that in some cases, Snort drops more packets in Linux 2.6 than in a virtual Linux, whereas, the same is not true with Suricata. Finally, it can be stated that Suricata performs well on Linux 2.6 as compared to FreeBSD and virtual Linux but fails to match Snort. Moreover, Suricata has a lower performance rate as compared to Snort despite having a multi-packet handling capability.

5.4.2 Scenario-2

The NIDP system can be implemented in either inside or outside the local network of organization. This decision is particularly made by the organization's network administrator depending upon security mechanisms. Regardless of how the sensor is placed, the NIDP system can provide a significant view into traffic crossing the network. The main objective of any NIDP system is to perform in-depth analysis of the traffic passing through the network and the achieved results can be helpful to any network administrator

to evaluate the network security state by reviewing the logs that show alerts of the intrusion attempts. On any given network, on any given day, NIDP system can fire thousands of alerts which make a challenging task for a network administrator to analyse all the data. For this purpose, metrics are considered as a valuable approach for network administrators to assess the security level of their networks.

Metrics has been used in many facets of a person's life especially in decision making process. The important questions related to network can be answered by these metrics, such as, is the network security level increasing or decreasing? Is NIDP system alarming on the correct events? which event should a network administrator focus on, etc. In order to create metrics, it is necessary for network administrator to determine that NIDP system is working as intended. Current NIDP systems like Snort has the capability to classify the alerts of impact of attacks in terms of high, medium, low and very low using common vulnerability scoring system (CVSS). To assess the security risk level of a network, these fuzzy values are not sufficient especially to analyse the network status in terms of attacks. Therefore, there is a need of new NIDP system security risk metrics, which should describe the network status in terms of the absolute value based on the alerts generated by NIDP systems quarterly, fortnightly or every day. Due to its good performance, Snort NIDP system is selected to assess the security risk level by analysing the number of alerts generated at traffic speeds 250Mbps, 500 Mbps, 750 Mbps, 1.0 Gbps, 1.5 Gbps and 2.0 Gbps for the designed test bench shown in Figure 5.3. For achieving consistency in the experiment,

the same number of rules (8,000) used in scenario-1 is applied to Scenario-2. Metasploit tool is used to generate malicious traffic from different nodes to the targeted NIDP system. Further, it is important to note that Linux OS is employed as NIDP systems perform well on it as observed from Scenario-1.

5.4.2.1 Attack Detection Rate (Alerts)

In order to see the effectiveness of Snort for different traffic speeds, a scenario is created with Metasploit tool generating malicious traffic towards the NIDP system. The results achieved in this analysis are given in Table 5.2.

Table 5.2: Snort behavior at different traffic speed.

Traffic Speed (per second)	Packet Analysed (%)	Packet Dropped (%)	Alerts generated by Snort (%)
250 Mb	100	0	100
500 Mb	100	0	100
750 Mb	100	0	100
1.0 Gb	100	0	100
1.5 Gb	100	0	100
2.0 Gb	86.4	13.6	99.7

It is clear from Table 5.2, Snort detects all the attacks until the speed reaches 1.5 Gbps. After this speed, 13.6% of the packets are dropped and, there is 0.3% inefficiency recorded in alert generation. This leads to defining

a threshold traffic speed for this scenario. It is also noted that Snort is capable to analyse all the packets and to generate alerts up to speed 1.5 Gbps. All the generated alerts are classified in terms of high, medium, low and very low severity levels using CVSS as given in Table 5.3.

Table 5.3: Classification of attacks defined in the Snort rule.

No	Class type	Description	No. of Alerts received	Priority
A1	Attempted-admin	Attempted Administrator Privilege Gain	229	High
A2	Attempted-user	Attempted User Privilege Gain	3	High
A3	Inappropriate-content	Inappropriate content was detected	0	-
A4	Policy-violation	Potential Corporate Privacy Violation	0	-
A5	Shellcode-detect	Executable code was detected	22	High
A6	Successful-admin	Successful Administrator Privilege Gain	0	-
A7	Successful-user	Successful User Privilege Gain	0	-
A8	Trojan-activity	A Network Trojan was	2	High

		detected		
A9	Unsuccessful-user	Unsuccessful User Privilege Gain	0	-
A10	Web-application attack	Web Application attack	58	High
A11	Attempted-dos	Attempted Denial of Service	141	Medium
A12	Attempted-recon	Attempted Information Leak	443	Medium
A13	Bad-unknown	Potentially Bad Traffic	0	-
A14	Default-login attempt	Attempt to login by a default username and password	1	Medium
A15	denial-of-service	Detection of a Denial of Service Attack	0	-
A16	Misc-attack	Misc Attack	6	Medium
A17	Non-standard-protocol	Detection of a non-standard protocol or event	1607	Medium
A18	rpc-portmap-decode	Decode of an RPC Query	0	-
A19	Successful-dos	Denial of Service	0	-

A20	Successful-recon large scale	Large Scale Information Leak	0	-
A21	Successful-recon limited	Information Leak	2206	Medium
A22	Suspicious-filename-detect	A suspicious filename was detected	0	-
A23	Suspicious-login	An attempted login using a suspicious username was detected	0	-
A24	System-call-detect	A system call was detected	0	-
A25	Unusual-client-port-connection	A client was using an unusual port	0	-
A26	Web-application activity	Access to a potentially vulnerable web application	18	Medium
A27	Icmp-event	Generic ICMP event	0	-
A28	Misc-activity	Misc Activity	20	Low
A29	Network-scan	Denial of a network Scan	0	-
A30	Not-suspicious	Not Suspicious Traffic	0	-
A31	Protocol-	Generic Protocol	0	-

	command-decode	Command Decode		
A32	String-detect	A suspicious string was detected	0	-
A33	Unknown	Unknown Traffic	0	-
A34	Tcp-connection	A TCP connection was detected	0	-

Now we are in a position to assess the security level of any organization by creating metrics based on the alerts to be generated by Snort. For this purpose, a total of 4756 alerts are generated against malicious traffic as shown in Figure 5.10.

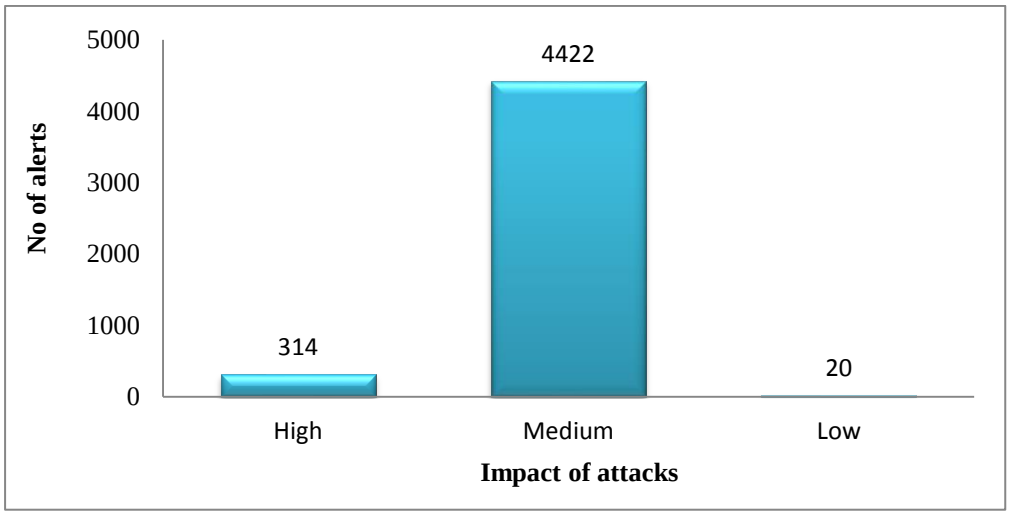

Figure 5.10: Total number of alerts based on attack impact.

From these alerts, 314 alerts belong to high priority, 4422 alerts having medium priority and the remaining 20 alerts are of low priority. There is no alerts of type very low priority (For detail, please see Appendix C). Since, the

information provided by alerts is of qualitative nature and therefore, it is not sufficient to determine the security level of a network whether it is improving or deteriorating. In this regard, security metrics can provide a better picture to a network administrator in assessing the security level quantitatively.

5.4.2.2 Evaluation Results

For assessing the quantitative security risk level of a network in terms of absolute value, the experimental study was carried out. Tests were conducted at various traffic speeds up to 1.5 Gbps using the test bench shown in Figure 5.3. The security level of a network is evaluated on the basis of two measured values: 1) different types of attack occurrences and 2) impacts of attack.

Case-1: Security level (SL) based on different types of attack occurrences

As can be seen in Table 5.3, the attacks are classified into 34 different categories on the basis of class types derived from the rules, where each class type is listed along with its description. The number of received alerts against each attack category is also specified in it. Assuming A_i, where $i \in \mathbb{Z}$ and $1 \leq i \leq 34$ is the ithattack generated against the network, and $SL(A_i)$ is the security level of a network due to A_i attack. Now, security level of a network based on type of attack is determined by the following expression:

$$SL(A_i) = \frac{\alpha_i}{\sum \alpha} \qquad (5.1)$$

Where α_i denotes the number of alerts generated against A_i and $\sum \alpha$ is the total number of received alerts against $\forall A_i$. Now using Table 5.3, $SL(.)$ are evaluated as

$$SL(A_1) = \frac{\alpha_1}{\sum \alpha} = \frac{229}{4756} = 4.8\% \quad (5.2)$$

$$SL(A_2) = \frac{\alpha_2}{\sum \alpha} = \frac{3}{4756} = 0.06\% \quad (5.3)$$

Similarly,$SL(A_3), SL(A_4)$, . . ., $SL(A_{34})$ are estimated, and are listed in Table 5.4.

Table 5.4: The security level of a network based on different types of attack occurrences.

SL **(A_i)**				
SL (A_1) = 4.8%	SL (A_2) = 0.06%	SL (A_3) = 0	SL (A_4) = 0	SL (A_5) = 0.5%
SL (A_6) = 0	SL (A_7) = 0	SL (A_8) = 0.04%	SL (A_9) = 0	SL (A_{10}) = 1.2%
SL (A_{11}) = 3%	SL (A_{12}) = 9.3%	SL (A_{13}) = 0	SL (A_{14}) = 0.02%	SL (A_{15}) = 0
SL (A_{16}) = 0.13%	SL (A_{17}) = 34%	SL (A_{18}) = 0	SL (A_{19}) = 0	SL (A_{20}) = 0
SL (A_{21}) = 46.4%	SL (A_{22}) = 0	SL (A_{23}) = 0	SL (A_{24}) = 0	SL (A_{25}) = 0
SL (A_{26}) = 0.4%	SL (A_{27}) = 0	SL (A_{28}) = 0.4%	SL (A_{29}) = 0	SL (A_{30}) = 0
SL (A_{31}) = 0	SL (A_{32}) = 0	SL (A_{33}) = 0	SL (A_{34}) = 0	

The security level of a network due to attack $A_1$is 4.8% as given by equation(5.2), which indicates that network is 95.2% secure against this attack. The security level due to attack A_2 is 0.06%, which implies that the network is 99.4% secure enough. Now consider the worst case, the security level is highest, i.e. 46.4% with respect to attack A_{21} as clear from Table 5.4.

It means that network is just 53.6% secure and sufficient countermeasures are required to mitigate the potential risks from it.

Case-2: Security level (SL) based on impact of attacks

For simplicity, let $high, medium, low$ and $verylow$ impacts of attack are represented by H, M, L and V respectively. It is important to note that these impacts or alerts are generated by Snort. As shown in Figure 5.10, $\sum H = 314$, $\sum M = 4422, \sum L = 20$ and $\sum V = 0$, as no alert is generated of this category. Suppose, $\sum H + \sum M + \sum L + \sum V = S$. Now, security level ($SL$) of a network based on impact is determined by the following expression:

$$SL(I_m) = \frac{\sum I_m}{S} \tag{5.4}$$

Where I_m denotes the particular impact category, $\sum I_m$ total alerts of I_m category, and S represents the total alerts of all impact categories. Now, plugging in the above values, the security levels of network against $high, medium, low$ and $verylow$ impacts of attack are as follows:

$$SL(H) = \frac{\sum H}{S} = \frac{314}{4756} = 6\% \tag{5.5}$$

$$SL(M) = \frac{\sum M}{S} = \frac{4422}{4756} = 93\% \tag{5.6}$$

$$SL(L) = \frac{\sum L}{S} = \frac{20}{4756} = 0.42\% \tag{5.7}$$

$$SL(V) = \frac{\sum V}{S} = 0\% \qquad \because \sum V = 0 \tag{5.8}$$

From equations 5.5-5.8, it is clear that security level of a network with respect to $high$ impact is 6%, which implies that network is 94% secure

enough against this impact. The security level against $medium$ impact of attack is 93%, which shows that network is just 7% secure and therefore, appropriate countermeasures need to be employed to secure it. The security level due to low impact is $0.42\%, i.e.\ (< 1\%)$, which indicates that network is 99% secure. However, it is not almost fully secure. Now, with respect to $very\ low$ impact of attack, the security level is zero. It means that the network is fully secure and, consequently, there are no threats of having $very\ low$ impact level.

5.4.2.3 Summary of Analysis

Based on performance, Snort NIDP system was employed to assess the security level of a network by analysing the alerts generated at various traffic speeds on the designed test bench. The security level was evaluated on the basis of different types of attack and the impacts of attack. The achieved security metrics describe the network status in terms of the absolute value which can help the network administrators in measuring the impact as well as the risk associated with each individual attack category.

Chapter 6.

CONCLUSIONS AND FUTURE WORK

In large organizations, network security has become a critical subject due to the frequent increase in their sizes and complexity. Since cybercrime has been commercialised, the tremendous amount of network resources in the enterprise environment provides a big pull for malicious attacks. The network security risk associated with each attack is directly proportional to how malicious the attack is. A successful attack on the network is defined by the ability to exploit the network vulnerabilities in order to compromise and intrude the network resources. In a small network, intrusion can be prevented using ordinary scanning tools, for example, firewalls and antivirus which only provide a snapshot of the system configuration and vulnerabilities at one time. Consequently, these tools are not appropriate to measure the security of enterprise networks. To accomplish this task at enterprise level, network intrusion detection and prevention (NIDP) systems are introduced for securing the network.

At present, the security community's major concern is to answer questions related to the vulnerability of a network or system. Some of the topics of interest are hardening network security with less effort, resources involved in a particular network, relationships among these resources and techniques used to achieve a specific target. All these efforts are utilised in securing a network but a little effort has been made towards measuring the overall security level of the enterprise network quantitatively. The objective of this

research is to provide a quantitative solution to the question regarding the overall security level of an organization. Some of the existing research is supported to answer this question by using the attack graph method that provides a way of measuring the risk associated with a successful exploitation of a combination of vulnerabilities. However, it does not give an absolute value. A metric providing an absolute value would help the network security teams in organizations in measuring the security of the network by several ways such as: they would be able to tell how an introduced application or software affects the security of the network as well as they would be able to measure how often affects the security of the same organization. The metric designed in this study can help the network security teams to answer such questions. Although the metric does not account for the human factor, rather, it uses the system vulnerabilities to give an absolute value of the network security risk assessment factor associated with cyber-attacks. In order to develop this metric, this work is focused on one of the major concerns, i.e. “How do we measure how secure the organizational network is from cyber-attacks?” This question has been broken down into smaller topics that can be exhaustively explored. Different types of vulnerabilities are explored and various types of cyber-attacks have been studied.

A UK based company was considered as a case study in the experiments carried out for both the known vulnerabilities and invisible attacks. Based on the results achieved from known vulnerabilities, a framework for the metrics was designed. For invisible attacks, the experiment was carried out to show

how these attacks were detected and mitigated. As different types of invisible attacks exist, this work is particularly focused on the impact of Google dorks. The results obtained from the effects of the invisible attacks were used for designing the rule, which then employed in the NIDP systems as a mitigation method. The metrics achieved from this case study can be applicable to any enterprise networking environment in order to define the overall security risk assessment absolute value of the organization.

Since NIDP systems were used at the enterprise level to shield the network against cyber-attacks, it was realised that there was a need to further explore these systems and propose a security risk metric. Two different NIDP systems were tested and compared in similar environments in order to find the most suitable system for the study. From the results based on the performance, Snort was chosen over Suricata. Using Snort, analysis was carried out in finding the maximum speeds at which no packet drops took place. Using this as test bench, security metrics measuring the absolute security level associated to the rules were developed; one to measure the impact while the other provides the risk associated with each individual attack category.

All these methods provide important features that can be exploited by the security community to improve the standards for measuring the network security level. Presently, the available standards showed qualitative security level which did not provide the best method to analyse and to present the overall security risk measure of an organization. The proposed methods provide enterprise network administrators with better measures and a clear

image of how secure their networks are. In order to further improve the metrics proposed in this work, the future work may address the following issues:

- Security risk associated with the inside attack; with this study focusing on the effect of the attacks from the outside world, the attacks from the inside of the organization were not considered. Inside factors such as human factor, system user factor, company internal policies factor, etc. should also be the scope for future research.
- Invisible attacks can be further explored in order to create a better generalised metric for this type of attack since this work focused on Google dorks based invisible attacks. For example, other forms of invisible attacks that can be examined are the Wi-Fi based invisible attacks and the possibility that other search engines have the same capability as the Google search engine. There is a possibility that other search engines have the capability to retrieve confidential information once the Google dorks based techniques are applied.
- The security risk level of a company can also be assessed by the ranking of the results related to the company when Google dorks are used to search for information. For example, a company is more vulnerable if its information shows up on the first page than one which shows up on other pages. This analysis can be used to develop a weighted metric that shows the company how susceptible it is to Google dork based attacks. A company which shows up on the first page has a higher risk weight than one that shows up on the other

pages. This information can be used to extend the functionality of the proposed risk assessment method for invisible attacks in this work.

- The developed metrics can also be linked with the attack graph tools to generate a system that automatically gives a detailed picture of the network security risk level while providing the overall absolute value of the security of the organization's network.
- This work focuses on the use of CVSS and OWASP rating methodology to design the quantitative security metrics. The format of developing the metric can be applied to different standards like IS1 among others to develop different metrics. The achieved metrics can be compared with the proposed metrics. These metrics can be presented to companies as different standards by which to quantitatively evaluate their network security risk level.

REFERENCES

[1] Chase, J., The Evolution of the Internet of Things. 2013, Dallas, TX: Texas Instruments Incorporated.

[2] Wilson, C. Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress, 2008. DTIC Document.

[3] Sicard, A. Security Threats Facing Enterprise Networks, 2013.

[4] Fyodor, D.F., SecTools.Org: Top 125 Network Security Tools, 2012.

[5] Al-Shaer, E., L. Khan, and M.S. Ahmed, A comprehensive objective network security metric framework for proactive security configuration, 2008, ACM.

[6] Holme, P., et al., Attack vulnerability of complex networks. Physical Review E, 2002, 65(5): p. 056109.

[7] Jajodia, S., S. Noel, and B. O'Berry, Topological analysis of network attack vulnerability, in Managing Cyber Threats, 2005, Springer. p. 247-266.

[8] Ou, X., W.F. Boyer, and M.A. McQueen, A scalable approach to attack graph generation, 2006, ACM.

[9] Noel, S., et al. Efficient minimum-cost network hardening via exploit dependency graphs, 2003, IEEE.

[10] Ou, X. and A. Singhal, Quantitative security risk assessment of enterprise networks, 2011: Springer.

[11] Ingols, K., R. Lippmann, and K. Piwowarski, Practical attack graph generation for network defence, 2006, IEEE.

[12] Lock, T. Is it possible to measure IT Security? 2010.

[13] Brito, H., M-Trends 2014 Threat Report Revealed, 2014.

[14] Eschelbeck, G., Security Threat Report 2014 Smarter, Shadier, Stealthier Malware, 2014.

[15] Cisco, Cisco 2014 Annual Security Report, 2014.

[16] GCHQ, Security and Information Risk Advice and Accreditation, N.T.A.f.I. Assurance, Editor, 2014.

[17] Maiwald, E., Fundamentals of network security. 2003: Dreamtech Press.

[18] Wang, A.J.A. Information security models and metrics. In Proceedings of the 43rd annual southeast regional conference-Volume 2. 2005. ACM.

[19] Maiwald, E., Network security: a beginner's guide. 2001: McGraw-Hill Professional.

[20] Peltier, T.R., Information security risk analysis. 2005: CRC press.

[21] Stallings, W. and L. Brown, Computer Security. 2008: Pearson Education.

[22] Moustafa, M.N., et al., QoS-enabled broadband mobile access to wireline networks. Communications Magazine, IEEE, 2002. 40(4): p. 50-56.

[23] Fung, K.T., Network security technologies. 2004: CRC Press.

[24] Mell, P., K. Scarfone, and S. Romanosky. A complete guide to the common vulnerability scoring system version 2.0. 2007.

[25] Liu, Q. and Y. Zhang, VRSS: A new system for rating and scoring vulnerabilities. Computer Communications, 2011. 34(3): p. 264-273.

[26] US-CERT, Untited States Computer Emergency Response Team, 2014 Bulletin. 2014.

[27] Alhomoud, A., et al., Performance Evaluation Study of Intrusion Detection Systems. Procedia Computer Science, 2011. 5: p. 173-180.

[28] TansuAlpcan, T.B., A decision and game theoretic approach. Ist ed. 2011: Cambridge University, UK.

[29] Mostafa, M., Analyse de sécuritéetQoSdans les réseaux à contraintestemporelles. 2011.

[30] Ingoldsby, T.R., Attack tree-based threat risk analysis. 2009, Calgary: Amenaza Technologies Limited.

[31] Schultz, E.E., A framework for understanding and predicting insider attacks. Computers & Security, 2002. 21(6): p. 526-531.

[32] Einwechter, N., Preventing and detecting insider attacks using ids. SecurityFocus, March, 2002.

[33] Tuglular, T. and E. Spafford, A framework for characterization of insider computer misuse. Unpublished paper, Purdue University, 1997.

[34] Ruppert, B., Protecting Against Insider Attacks 2009.

[35] Wilson, C., Computer attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress. Cyberterrorism And Computer Attacks, 2003: p. 1-59.

[36] Fernández-Muñiz, B., J.M. Montes-Peón, and C.J. Vázquez-Ordás, Occupational risk management under the OHSAS 18001 standard: analysis of perceptions and attitudes of certified firms. Journal of Cleaner Production, 2012. 24: p. 36-47.

[37] Payne, S.C., A guide to security metrics. SANS Institute Information Security Reading Room, 2006.

[38] PATRICIU, V.-V., SECURITY METRICS FOR ENTERPRISE INFORMATION SYSTEMS. 2006.

[39] Wang, L., et al., k-Zero day safety: A network security metric for measuring the risk of unknown vulnerabilities. 2014.

[40] Kumar, V., J. Srivastava, and A. Lazarević, Managing cyber threats: issues, approaches, and challenges. Vol. 5. 2005: Springer Verlag.

[41] Antonatos, S., et al. Performance analysis of content matching intrusion detection systems. 2004. IEEE.

[42] Anderson, J.P., Computer security threat monitoring and surveillance. 1980.

[43] Liu, Z.Y.M. Intrusion Detection Systems. in Applied Mechanics and Materials. 2014.

[44] Tenable. Nessus, The global standard in detecting and assessing network data. 1998 26/04/2014]; Available from: http://www.tenable.com/products/nessus.

[45] Vulnerability Management. [cited 30/04/2012; Available from: http://www.rapid7.com/products/vulnerability-management.jsp.

[46] Lyon, G., Top 100 Network security tools. SecTools. Org, 2006.

[47] Holm, H., A Framework and Calculation Engine for Modeling and Predicting the Cyber Security of Enterprise Architectures. 2014.

[48] Phillips, C. and L.P. Swiler. A graph-based system for network-vulnerability analysis. in Proceedings of the 1998 workshop on New security paradigms. 1998. ACM.

[49] Schneier, B., Attack trees. Dr. Dobb's journal, 1999. 24(12): p. 21-29.

[50] Dacier, M., Y. Deswarte, and M. Kaâniche, Models and tools for quantitative assessment of operational security. 1996.

[51] Frigault, M., et al. Measuring network security using dynamic bayesian network. 2008. ACM.

[52] Swiler, L.P., et al. Computer-attack graph generation tool. in DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings. 2001. IEEE.

[53] Proact. ISS System Scanner. 1994 05/06/2014]; Available from: http://www.tech.proact.co.uk/iss/iss_system_scanner.htm.

[54] X-Force, I. CyberCop by Network Associates. 1998.

[55] Biere, A., et al., Symbolic model checking without BDDs. 1999: Springer.

[56] Ritchey, R.W. and P. Ammann. Using model checking to analyze network vulnerabilities. 2000. IEEE.

[57] Amenazahttp://www.amenaza.com/AT-whatAre.php. 2001.

[58] Sheyner, O. and J. Wing, Toward compositional analysis of security protocols using theorem proving. 2000, DTIC Document.

[59] Sheyner, O., et al. Automated generation and analysis of attack graphs. 2002. IEEE.

[60] Sheyner, O. and J. Wing. Tools for generating and analyzing attack graphs. 2004. Springer.

[61] Ou, X., W.F. Boyer, and M.A. McQueen. A scalable approach to attack graph generation. in Proceedings of the 13th ACM conference on Computer and communications security. 2006. ACM.

[62] Homer, J. and X. Ou, SAT-solving approaches to context-aware enterprise network security management. Selected Areas in Communications, IEEE Journal on, 2009. 27(3): p. 315-322.

[63] Homer, J., et al., Aggregating vulnerability metrics in enterprise networks using attack graphs. Journal of Computer Security, 2013. 21(4): p. 561-597.

[64] Huang, H., et al. Distilling critical attack graph surface iteratively through minimum-cost sat solving. in Proceedings of the 27th Annual Computer Security Applications Conference. 2011. ACM.

[65]Wang, L., A. Singhal, and S. Jajodia. Toward measuring network security using attack graphs. 2007. ACM.

[66] Li, Z., et al. A data mining approach to generating network attack graph for intrusion prediction. 2007. IEEE.

[67] Chen, F., et al., An atomic-domains-based approach for attack graph generation. World Academy of Science, Engineering and Technology, 2009. 56: p. 775-781.

[68] Liu, Y. and H. Man. Network vulnerability assessment using Bayesian networks. 2005.

[69] Xie, P., et al. Using Bayesian networks for cyber security analysis. 2010. IEEE.

[70] Jajodia, S. and S. Noel, Topological vulnerability analysis, in Cyber Situational Awareness. 2010, Springer. p. 139-154.

[71] Fifield, F.a.D. Nexpose Vulnerability Scanner. 2011; Available from: http://sectools.org/tag/vuln-scanners/.

[72] Mell, P., K. Scarfone, and S. Romanosky. A complete guide to the common vulnerability scoring system version 2.0. in Published by FIRST-Forum of Incident Response and Security Teams. 2007.

[73] Wang, J., M. Xia, and F. Zhang, Metrics for information security vulnerabilities. Journal of Applied Global Research, 2008. 1(1): p. 48-58.

[74] Spain, S. Common Vulnerability Scoring System. 2014.

[75] Singhal, A. and X. Ou, Security risk analysis of enterprise networks using probabilistic attack graphs. 2011: Citeseer.

[76] Munir, R., et al. A Quantitative Measure of the Security Risk Level of Enterprise Networks. in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on. 2013. IEEE.

[77] Lyon, G. Top 125 Network Security Tools. 2011,[29/04/2014]; Available from: http://sectools.org/tool/retina/#comments.

[78] Kundi, G.M., Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries. Journal of Information Engineering and Applications, 2014. 4(4): p. 61-70.

[79] Paganinip US Crititcal Infrastructure under unceasing cyber attacks. 2013.

[80] labs, W.s., Websense 2014 threat report. 2014.

[81] Wilhoit, K., Who's Really Attacking Your ICS Equipment? Trend Micro, 2013.

[82] Oh, O., et al. An exploration of unintended online private information disclosure in educational institutions across four countries. ineCrime Researchers Summit, 2009. eCRIME'09. 2009. IEEE.

[83] Abdelhalim, A. and I. Traore. The impact of google hacking on identity and application fraud. in Pacific Rim Conference on Communications, Computers and Signal Processing. 2007. Citeseer.

[84] Roesch, M. and C. Green, Snort users manual snort release: 2.0. 1. Snort Documentation, 2003.

[85] Alserhani, F., et al. Evaluating Intrusion Detection Systems in High Speed Networks. 2009. IEEE.

[86] Munir, R., Performance analysis of IDS (Snort). 2009.

[87] Caswell, B., J. Beale, and A. Baker, Snort Intrusion Detection and Prevention Toolkit. 2007: Elsevier.

[88] Beale, J., et al., Snort: IDS and IPS toolkit. 2007: Syngress Media Inc.

[89] SPAWAR. Suricata. 2010; Available from:https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_User_Guide.

[90] Lowe, S., Mastering VMware vSphere 4. 2009: Sybex.

[91] ABDALLAH, A. and T. HASSAN, Formalizing Delegation and Integrating it into Role-Based Access Control Models. Journal of Information Assurance and Security, 2010. 5: p. 021-030.

APPENDIX A: CLASSIFICATION OF VULNERABILITIES

This shows a sample of the vulnerabilities that were collected after scanning the case study company network using Nexpose Vulnerability scanning tool.

Exposures: Susceptible to malware attacks | Metasploit-exploitable | Exploit published

Title	CVSS	Risk	Published On	Severity	Instances	Exceptions
APSB11-18: Security update available for Adobe Flash Player (CVE-2011-2110)	10	919	Tue Jun 14 2011	Critical	1	Exclude
APSB12-01: Security updates available for Adobe Reader and Acrobat (CVE-2011-2462)	10	919	Wed Dec 07 2011	Critical	1	Exclude
Adobe Flash Player Unspecified Vulnerability On Opera Browser For Mac OS X	10	818	Tue Dec 18 2007	Critical	1	Exclude
Windows DLL Hijacking Vulnerability	10	749	Mon Aug 23 2010	Critical	1	Exclude
APSB12-08: Security updates available for Adobe Reader and Acrobat (CVE-2012-0775)	10	727	Tue Apr 10 2012	Critical	1	Exclude
APSB11-21: Security update available for Adobe Flash Player (CVE-2011-2134)	10	715	Tue Aug 09 2011	Critical	1	Exclude
APSB11-21: Security update available for Adobe Flash Player (CVE-2011-2425)	10	715	Tue Aug 09 2011	Critical	1	Exclude
APSB11-21: Security update available for Adobe Flash Player (CVE-2011-2135)	10	715	Tue Aug 09 2011	Critical	1	Exclude
APSB11-21: Security update available for Adobe Flash Player (CVE-2011-2137)	10	715	Tue Aug 09 2011	Critical	1	Exclude
APSB11-21: Security update available for Adobe Flash Player (CVE-2011-2136)	10	715	Tue Aug 09 2011	Critical	1	Exclude
APSB11-21: Security update available for Adobe Flash Player (CVE-2011-2130)	10	715	Tue Aug 09 2011	Critical	1	Exclude
APSB12-03: Security update available for Adobe Flash Player (CVE-2012-0754)	10	706	Thu Feb 16 2012	Critical	1	Exclude
APSB11-28: Security update available for Adobe Flash Player (CVE-2011-2460)	10	704	Fri Nov 11 2011	Critical	1	Exclude
APSB11-28: Security update available for Adobe Flash Player (CVE-2011-2453)	10	704	Fri Nov 11 2011	Critical	1	Exclude
APSB11-28: Security update available for Adobe Flash Player (CVE-2011-2452)	10	704	Fri Nov 11 2011	Critical	1	Exclude
APSB11-28: Security update available for Adobe Flash Player (CVE-2011-2451)	10	704	Fri Nov 11 2011	Critical	1	Exclude
APSB11-28: Security update available						

APSB11-28: Security update available for Adobe Flash Player (CVE-2011-2456)			10	704	Fri Nov 11 2011	Critical	1 Exclude
APSB11-28: Security update available for Adobe Flash Player (CVE-2011-2457)			10	704	Fri Nov 11 2011	Critical	1 Exclude
APSB12-01: Security updates available for Adobe Reader and Acrobat (CVE-2011-4369)			10	700	Fri Dec 16 2011	Critical	1 Exclude
APSB12-03: Security update available for Adobe Flash Player (CVE-2012-0753)			10	693	Thu Feb 16 2012	Critical	1 Exclude
APSB12-03: Security update available for Adobe Flash Player (CVE-2012-0756)			10	693	Thu Feb 16 2012	Critical	1 Exclude
APSB12-03: Security update available for Adobe Flash Player (CVE-2012-0755)			10	693	Thu Feb 16 2012	Critical	1 Exclude
APSB12-03: Security update available for Adobe Flash Player (CVE-2012-0751)			10	693	Thu Feb 16 2012	Critical	1 Exclude
APSB12-03: Security update available for Adobe Flash Player (CVE-2012-0752)			10	693	Thu Feb 16 2012	Critical	1 Exclude
APSB12-05: Security update available for Adobe Flash Player (CVE-2012-0768)			10	691	Mon Mar 05 2012	Critical	1 Exclude
APSB12-07: Security update available for Adobe Flash Player (CVE-2012-0773)			10	688	Wed Mar 28 2012	Critical	1 Exclude
APSB12-07: Security update available for Adobe Flash Player (CVE-2012-0772)			10	688	Wed Mar 28 2012	Critical	1 Exclude
APSB12-07: Security update available for Adobe Flash Player (CVE-2012-0724)			10	687	Fri Apr 06 2012	Critical	1 Exclude
APSB12-07: Security update available for Adobe Flash Player (CVE-2012-0725)			10	687	Fri Apr 06 2012	Critical	1 Exclude
APSB12-08: Security updates available for Adobe Reader and Acrobat (CVE-2012-0774)			10	687	Tue Apr 10 2012	Critical	1 Exclude
APSB12-08: Security updates available for Adobe Reader and Acrobat (CVE-2012-0776)			10	687	Tue Apr 10 2012	Critical	1 Exclude
APSB12-14: Security updates available for Adobe Flash Player (CVE-2012-2037)			10	679	Fri Jun 08 2012	Critical	1 Exclude
APSB12-14: Security updates available for Adobe Flash Player (CVE-2012-2035)			10	679	Fri Jun 08 2012	Critical	1 Exclude

APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2012-1530)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0601)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0602)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0603)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0604)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0605)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0606)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0607)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0608)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0609)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0610)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-01: Security updates available for Adobe Flash Player (CVE-2013-0630)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0611)			10	651	Tue Jan 08 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-1366)			10	646	Tue Feb 12 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-0644)			10	646	Tue Feb 12 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-0639)			10	646	Tue Feb 12 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-1374)			10	646	Tue Feb 12 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-1372)			10	646	Tue Feb 12 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-1370)			10	646	Tue Feb 12 2013	Critical	1 Exclude
APSB13-05: Security updates available for Adobe Flash Player (CVE-2013-1373)			10	646	Tue Feb 12 2013	Critical	1 Exclude

MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution			9.3	321	Tue Dec 11 2012	Critical	1	Exclude
APSB13-04: Security updates available for Adobe Flash Player (CVE-2013-0634)			9.3	321	Thu Feb 07 2013	Critical	1	Exclude
MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution			9.3	312	Tue Jan 08 2013	Critical	1	Exclude
APSB13-04: Security updates available for Adobe Flash Player (CVE-2013-0633)			9.3	302	Thu Feb 07 2013	Critical	1	Exclude
APSB13-07: Security updates available for Adobe Reader and Acrobat (CVE-2013-0640)			9.3	300	Wed Feb 13 2013	Critical	1	Exclude
APSB13-07: Security updates available for Adobe Reader and Acrobat (CVE-2013-0641)			9.3	300	Wed Feb 13 2013	Critical	1	Exclude
APSB13-08: Security updates available for Adobe Flash Player (CVE-2013-0648)			9.3	296	Tue Feb 26 2013	Critical	1	Exclude
APSB13-08: Security updates available for Adobe Flash Player (CVE-2013-0643)			9.3	296	Tue Feb 26 2013	Critical	1	Exclude
Password password on CIFS Administrator account			7.5	908	Wed Jan 01 1997	Critical	1	Exclude
CIFS NULL Session Permitted			7.5	750	Wed Jan 01 1997	Critical	1	Exclude
IRDP (ICMP Router Discovery Protocol) enabled			7.5	743	Wed Aug 11 1999	Critical	1	Exclude
IP Source Routing Enabled			7.5	743	Mon Sep 20 1999	Critical	1	Exclude
APSB12-01: Security updates available for Adobe Reader and Acrobat (CVE-2011-4372)			7.5	577	Tue Jan 10 2012	Critical	1	Exclude
APSB12-01: Security updates available for Adobe Reader and Acrobat (CVE-2011-4371)			7.5	577	Tue Jan 10 2012	Critical	1	Exclude
APSB12-01: Security updates available for Adobe Reader and Acrobat (CVE-2011-4373)			7.5	577	Tue Jan 10 2012	Critical	1	Exclude
APSB12-01: Security updates available for Adobe Reader and Acrobat (CVE-2011-4370)			7.5	577	Tue Jan 10 2012	Critical	1	Exclude
APSB11-24: Security updates available for Adobe Reader and Acrobat (CVE-2011-4374)			7.5	576	Thu Jan 19 2012	Critical	1	Exclude
APSB12-08: Security updates available for Adobe Reader and Acrobat (CVE-2012-0777)			7.5	568	Tue Apr 10 2012	Critical	1	Exclude
APSB12-16: Security update available for Adobe Reader and Acrobat (CVE-2012-4162)			7.5	555	Wed Aug 15 2012	Critical	1	Exclude
APSB12-16: Security update available for Adobe Reader and Acrobat (CVE-2012-4161)			7.5	555	Wed Aug 15 2012	Critical	1	Exclude
CIFS Minimum Password Length Policy Not Enforced			6.8	786	Mon Nov 01 2004	Severe	1	Exclude

Adobe Flash Arbitrary Filesystem Traversal Vulnerability			7.1	476	Thu Dec 10 2009	Severe	1 Exclude
APSB10-07: Security updates available for Adobe Reader and Acrobat (CVE-2010-0186)			6.8	473	Mon Feb 15 2010	Severe	1 Exclude
APSB10-06 and APSB10-07: Adobe Reader and Flash Cross Domain Sandbox Restriction Bypass			6.8	473	Tue Feb 16 2010	Severe	1 Exclude
APSB10-15: Security updates available for Adobe Reader and Acrobat (CVE-2010-2203)			6.8	452	Wed Jun 30 2010	Severe	1 Exclude
APSB11-03: Security updates available for Adobe Reader and Acrobat (CVE-2011-0605)			6.8	413	Thu Feb 10 2011	Severe	1 Exclude
APSB11-03: Security updates available for Adobe Reader and Acrobat (CVE-2011-0568)			6.8	413	Thu Feb 10 2011	Severe	1 Exclude
APSB11-02: Security update available for Adobe Flash Player (CVE-2011-0575)			6.9	395	Tue Feb 08 2011	Severe	1 Exclude
APSB11-03: Security updates available for Adobe Reader and Acrobat (CVE-2011-0570)			6.9	395	Thu Feb 10 2011	Severe	1 Exclude
APSB11-03: Security updates available for Adobe Reader and Acrobat (CVE-2011-0562)			6.9	395	Thu Feb 10 2011	Severe	1 Exclude
APSB11-03: Security updates available for Adobe Reader and Acrobat (CVE-2011-0588)			6.9	395	Thu Feb 10 2011	Severe	1 Exclude
APSB11-16: Security updates available for Adobe Reader and Acrobat (CVE-2011-2100)			6.9	359	Thu Jun 16 2011	Severe	1 Exclude
APSB11-24: Security updates available for Adobe Reader and Acrobat (CVE-2011-1353)			6.9	332	Thu Sep 15 2011	Severe	1 Exclude
APSB12-14: Security updates available for Adobe Flash Player (CVE-2012-2040)			7.2	313	Fri Jun 08 2012	Severe	1 Exclude
APSB13-02: Security updates for Adobe Reader and Acrobat (CVE-2013-0627)			7.2	240	Tue Jan 08 2013	Severe	1 Exclude
SMB signing not required			6.2	723	Mon Nov 01 2004	Severe	2 Exclude
APSB11-12: Security update available for Adobe Flash Player (CVE-2011-0579)			5	473	Thu May 12 2011	Severe	1 Exclude
APSB09-10: Security updates available for Adobe Flash Player (CVE-2009-1870)			4.9	465	Fri Jul 31 2009	Severe	1 Exclude
APSB11-26: Security update available for Adobe Flash Player (CVE-2011-			5	464	Wed Sep 21 2011	Severe	1 Exclude

APPENDIX B: INVISIBLE ATTACKS

This shows a sample of the google dorks commands that can be used as invisible attacks for various purposes.

inurl:ocw_login_username

"Login to Usermin" inurl:20000

intitle:"OnLine Recruitment Program - Login"

intitle:"MailMan Login"

intitle:"phpPgAdmin - Login" Language

intitle:"EXTRANET login" -.edu -.mil -.gov

intitle:"ePowerSwitch Login"

intitle:"Employee Intranet Login"

intitle:rapidshareintext:login

inurl:orasso.wwsso_app_admin.ls_login

inurl:ocw_login_username

inurl:metaframexp/default/login.asp | intitle:"Metaframe XP Login"

inurl:cgi-bin/ultimatebb.cgi?ubb=login

inurl:coranto.cgiintitle:Login (Authorized Users Only)

intitle:"DocutekERes - Admin Login" -edu

intitle:"Admin Login" "admin login" "blogware"

intext:"Master Account" "Domain Name" "Password" inurl:/cgi-bin/qmailadmin

intext:"Storage Management Server for" intitle:"Server Administration"

intitle:"Admin login" "Web Site Administration" "Copyright"

intitle:"ColdFusion Administrator Login"

intitle:"Icecast Administration Admin Page"

intitle:"ListMail Login" admin -demo

intitle:adminintitle:login

inurl:"wvdial.conf" intext:"password"

intitle:rapidshareintext:login

filetype:loginurl:"password.log"

Please enter a valid password! inurl:polladmin

admin account info" filetype:log

Inurl:zebra.confintext:password -sample -test -tutorial -download

filetype:configconfigintext:appSettings "User ID"

filetype:incmysql_connect OR mysql_pconnect

filetype:sql password

Filetype:regreg +intext:"defaultusername" +intext:"defaultpassword"

Inurl:"editor/list.asp" | inurl:"database_editor.asp" | inurl:"login.asa" "are set"

Inurl:chap-secrets -cvs

Inurl:ventrilo_srv.ini adminpassword

Inurl:"slapd.conf" intext:"rootpw" -manpage -"Manual Page" -man: -

sample

Inurl:"wvdial.conf" intext:"password"

Inurl:ospfd.confintext:password -sample -test -tutorial -download

filetype:bltblt +intext:screenname

ext:reg "username=*" putty

inurl:/cgi-bin/pass.txt

inurl:preferences.ini "[emule]"

enable password | secret "current configuration" -intext:the

ext:asa | ext:bakintext:uidintext:pwd -"uid..pwd" database | server | dsn

ext:aspinurl:pathto.asp

ext:log "Software: Microsoft Internet Information Services *.*"

filetype:infinurl:capolicy.inf

filetype:emleml +intext:"Subject" +intext:"From" +intext:"To"

APPENDIX C: ALERT GENERATED BY NIDP SYSTEM

A list of alerts generated by NIDP system (Snort) during the case study. These are the alerts that were used to formulate the different security level (SL) metrics in this study.

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/08-12:39:18.352973 10.1.70.131:58530 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:162

AP Seq: 0x13A0B57F Ack: 0x36DB9B03 Win: 0x200 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:13816:1] SPECIFIC THREAT Metasploit Framework xmlrpc.php command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/08-13:02:42.105108 10.2.190.254:51273 -> 154.241.88.201:80

TCP TTL:61 TOS:0x0 ID:47330 IpLen:20 DgmLen:1200 DF

A* Seq: 0x59CF46AF Ack: 0xF50ED3B0 Win: 0xB7 TcpLen: 32

TCP Options (3) => NOP NOP TS: 917151 77829724

[Xref =>http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-1921]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/10-12:01:37.594862 10.2.23.225:49793 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:155

AP Seq: 0xEFAAAD5B Ack: 0x6F760D03 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:13819:1] WEB-MISC IBM Lotus Domino Web Server Accept-Language header buffer overflow attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/10-12:46:14.909643 10.2.200.229:55728 -> 154.241.88.201:80

TCP TTL:61 TOS:0x0 ID:61593 IpLen:20 DgmLen:328 DF

AP Seq: 0xC34B707 Ack: 0xD601D983 Win: 0x16D TcpLen: 32

TCP Options (3) => NOP NOP TS: 1001342 148947698

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-2240][Xref =>http://www.securityfocus.com/bid/29310]

[**] [1:13819:1] WEB-MISC IBM Lotus Domino Web Server Accept-Language header buffer overflow attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/10-12:46:18.143767 10.2.200.229:37764 -> 154.241.88.201:80

TCP TTL:61 TOS:0x0 ID:21554 IpLen:20 DgmLen:1096 DF

AP Seq: 0xEC81DCD Ack: 0xD872D8A7 Win: 0x16D TcpLen: 32

TCP Options (3) => NOP NOP TS: 1002158 148950919

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-2240][Xref =>http://www.securityfocus.com/bid/29310]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:00.982165 10.2.23.169:48509 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x148E8E60 Ack: 0xE758FBA8 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:05.996616 10.2.23.167:39951 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x1923212A Ack: 0xABE6B221 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:10.970311 10.2.23.231:59757 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x1DE96CDD Ack: 0xDA71BB2A Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:15.975006 10.2.23.122:44827 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x226EBB65 Ack: 0xCF5B121 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:20.999265 10.2.23.136:60613 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x274BE122 Ack: 0xD94AD8A1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:25.941717 10.2.23.251:42216 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x2B5D09E5 Ack: 0x95CF82B Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:30.950271 10.2.23.115:37212 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x301493CC Ack: 0xEE3E1EAB Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:35.947788 10.2.23.47:55618 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x354691DD Ack: 0xA744AFA1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:40.936833 10.2.23.193:49319 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x39C4A233 Ack: 0xAE8D4429 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:45.932408 10.2.23.252:56221 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x3E771449 Ack: 0x593C8A7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:50.990288 10.2.23.37:33691 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x430C34DC Ack: 0x57E70FA7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:45:56.047270 10.2.23.183:32881 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x4768C3C8 Ack: 0x7E86E1A1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:01.020204 10.2.23.225:33017 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x4C8D3786 Ack: 0xE3554625 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:06.048755 10.2.23.220:46391 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x509D254C Ack: 0xE33850AA Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:11.009707 10.2.23.184:47388 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x55421506 Ack: 0xCB20CBA5 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:21.000332 10.2.23.127:42794 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x5F152080 Ack: 0x326B71A9 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:25.997881 10.2.23.189:45442 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x6436390D Ack: 0xA2D57229 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:31.078430 10.2.23.0:43064 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x68C2A49F Ack: 0xF4EBA929 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.030465 10.2.23.220:46403 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x6D87D840 Ack: 0x1060ABAB Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.032120 10.2.23.220:46404 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:176

AP Seq: 0x6CD60D09 Ack: 0x3F896D29 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.032724 10.2.23.220:46406 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:182

AP Seq: 0x6D9EDD8D Ack: 0x5B54E6B1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.033605 10.2.23.220:46405 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:170

AP Seq: 0x6CE5F0FB Ack: 0xCB6A6FA7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.069487 10.2.23.220:46408 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:177

AP Seq: 0x6D51896A Ack: 0xADD25DAC Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.070277 10.2.23.220:46407 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x6CD7481E Ack: 0x65995A20 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.361276 10.2.23.220:46411 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:190

AP Seq: 0x6D7693D4 Ack: 0x1F92EBA9 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.357046 10.2.23.220:46409 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:178

AP Seq: 0x6D7FBC48 Ack: 0x1C8F76A7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:36.365238 10.2.23.220:46410 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:171

AP Seq: 0x6D8BDBB7 Ack: 0x194B61B Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:41.176267 10.2.23.8:58559 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:163

AP Seq: 0x71F38594 Ack: 0x1DB0CC18 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:46.138434 10.2.23.96:56736 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x76D04146 Ack: 0x6C45A61E Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref => http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:51.085691 10.2.23.135:39449 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x7B960381 Ack: 0x460A1FA5 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:46:56.055609 10.2.23.162:33627 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x7F77DF5E Ack: 0xE9C1E2A6 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:01.156458 10.2.23.18:56395 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x84D52A46 Ack: 0x5D5A14A3 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:06.070262 10.2.23.135:39455 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x88FFFA78 Ack: 0x6A1B2C25 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:11.092987 10.2.23.125:50495 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x8E0B8DF9 Ack: 0xD6D664A5 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:16.072708 10.2.23.189:45470 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x922353E2 Ack: 0x49F8D3A6 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING [**]

[Priority: 3]

11/11-09:47:37.332215 10.2.23.189:55531 -> 154.241.88.201:80

TCP TTL:61 TOS:0x0 ID:15987 IpLen:20 DgmLen:417 DF

AP Seq: 0xA69FDE8D Ack: 0x7DD9F954 Win: 0xB7 TcpLen: 32

TCP Options (3) => NOP NOP TS: 6349062 224644212

[**] [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING [**]

[Priority: 3]

11/11-09:47:38.635226 10.2.23.189:55533 -> 154.241.88.201:80

TCP TTL:61 TOS:0x0 ID:38833 IpLen:20 DgmLen:690 DF

AP Seq: 0xA77975EE Ack: 0x7F110A99 Win: 0xB7 TcpLen: 32

TCP Options (3) => NOP NOP TS: 6349389 224645513

[**] [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING [**]

[Priority: 3]

11/11-09:47:39.950385 10.2.23.189:55535 -> 154.241.88.201:80

TCP TTL:61 TOS:0x0 ID:17254 IpLen:20 DgmLen:758 DF

AP Seq: 0xA8B5A0EE Ack: 0x80B7A7CD Win: 0xB7 TcpLen: 32

TCP Options (3) => NOP NOP TS: 6349718 224646826

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:40.707137 10.2.23.160:32867 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xA9AFD4B7 Ack: 0xD99EBCA7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:50.685040 10.2.23.251:42287 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xB2A3C871 Ack: 0xE477C1AB Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:47:55.622888 10.2.23.43:35565 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xB7BEF602 Ack: 0xFB33BFAB Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:00.622985 10.2.23.147:47750 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xBC4F08AF Ack: 0x149FC79F Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:05.643484 10.2.23.120:57019 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xC1507F7D Ack: 0xA7153628 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:10.678998 10.2.23.38:52217 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xC5D910E1 Ack: 0x7BBE120 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:15.714935 10.2.23.246:36213 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xCAE31ACD Ack: 0xBFF1211D Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:20.691872 10.2.23.252:56336 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xCF6EF28A Ack: 0xFA631C1F Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:35.790562 10.2.23.185:35803 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xDD056F91 Ack: 0xE20D57AB Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:40.782599 10.2.23.2:51228 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xE239F00A Ack: 0x90CA49A6 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:45.756997 10.2.23.252:56375 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xE69B1618 Ack: 0x5EF06620 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:50.745404 10.2.23.140:34364 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xEB9659DD Ack: 0x997FCC23 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:55.697047 10.2.23.158:33538 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xEFF0E8E2 Ack: 0x84725CA4 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:00.757175 10.2.23.27:49708 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xF4EBF6D7 Ack: 0x2392511D Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:05.671017 10.2.23.16:46736 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xF959FED6 Ack: 0xBDC0CA7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:10.720977 10.2.23.219:50201 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xFE05FB97 Ack: 0x34DC8228 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:15.685464 10.2.23.213:50871 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x2CA8572 Ack: 0x75B5D4AA Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:20.652045 10.2.23.15:56035 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x7AFC16D Ack: 0x6A7BBC1E Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:25.702889 10.2.23.119:55634 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xD28B9E6 Ack: 0xF3A6939D Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:30.657457 10.2.23.202:42093 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x11CB76E1 Ack: 0x23A71820 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:35.654151 10.2.23.63:35416 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x163B01EB Ack: 0xEB23FF28 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:48:25.646206 10.2.23.22:55629 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0xD3577B7D Ack: 0x2CF1041E Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:46.268776 10.2.23.87:53471 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x1F52DFE0 Ack: 0x8F74F7AB Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:50.693059 10.2.23.169:47295 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x23F994D0 Ack: 0x6D9AC1A9 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:49:55.702015 10.2.23.55:42321 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x293DBAF4 Ack: 0x251ED22A Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:50:00.705414 10.2.23.122:41807 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x2DB291A1 Ack: 0x5531502B Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:50:05.757625 10.2.23.61:33700 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x3201EF1E Ack: 0x54942429 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:50:10.688385 10.2.23.219:53971 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x377FAE4B Ack: 0xA5197A9C Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:50:15.705661 10.2.23.194:36743 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x3C3F93E5 Ack: 0x876A4029 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:01.138888 10.2.23.6:48282 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x7FE348A8 Ack: 0x9ACED59F Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:11.161773 10.2.23.162:56092 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x8904633F Ack: 0x45AB8A1E Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:16.129100 10.2.23.24:58063 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x8E12DEA0 Ack: 0xCBD361A9 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:21.150288 10.2.23.143:33266 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x92A7C645 Ack: 0xEC874823 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:26.115250 10.2.23.185:34447 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x972BFE64 Ack: 0x65F0EB26 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:31.168447 10.2.23.50:32941 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x9C59451D Ack: 0x5FDB739E Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.553768 10.2.23.50:32942 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x9E0E63D1 Ack: 0xFCF33628 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.555563 10.2.23.50:32944 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x9DEDDB11 Ack: 0xE05BE7AA Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.554753 10.2.23.50:32945 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x9E276AAF Ack: 0xA2C213AA Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.615027 10.2.23.50:32946 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x9E399EA2 Ack: 0x5D2915A6 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.616333 10.2.23.50:32947 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:176

AP Seq: 0x9EA2BDF7 Ack: 0xBC853EAC Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.556441 10.2.23.50:32943 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:169

AP Seq: 0x9DE961C0 Ack: 0x74B609A6 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.988449 10.2.23.50:32948 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9EB91A3D Ack: 0x64DF74A1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.995962 10.2.23.50:32949 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9E9FF02D Ack: 0x93A37D25 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.992612 10.2.23.50:32951 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9E57DDE7 Ack: 0xC6FD6C1D Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.989807 10.2.23.50:32952 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9F310F5C Ack: 0x8114DA23 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.990820 10.2.23.50:32950 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9E701BE0 Ack: 0x16DC2DA1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.043814 10.2.23.50:32955 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9E9BA415 Ack: 0xC56ECDA1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:33.993816 10.2.23.50:32953 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9E687DEB Ack: 0x7686DD9F Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.042861 10.2.23.50:32954 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9EE96BDA Ack: 0x5DC3B9A1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.098795 10.2.23.50:32956 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9F262E9D Ack: 0x44C51B9F Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.098298 10.2.23.50:32957 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9F0EAEE6 Ack: 0x99CB5C25 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.161794 10.2.23.50:32959 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9ECCD1B0 Ack: 0x119009B Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.104116 10.2.23.50:32958 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9E6D8A14 Ack: 0xB266C91B Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.310569 10.2.23.50:32951 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9E57DED0 Ack: 0xC6FD6D4F Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.325475 10.2.23.50:32948 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9EB91B26 Ack: 0x64DF75D3 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.325860 10.2.23.50:32950 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:287

AP Seq: 0x9E701CC9 Ack: 0x16DC2ED3 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.334116 10.2.23.50:32949 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9E9FF116 Ack: 0x93A37E57 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.364865 10.2.23.50:32953 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9E687ED4 Ack: 0x7686DED1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.336341 10.2.23.50:32955 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:280

AP Seq: 0x9E9BA4FE Ack: 0xC56ECED3 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.352390 10.2.23.50:32952 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:280

AP Seq: 0x9F311045 Ack: 0x8114DB5C Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.379373 10.2.23.50:32954 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9EE96CC3 Ack: 0x5DC3BAD3 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.400220 10.2.23.50:32956 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9F262F86 Ack: 0x44C51CD1 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.417656 10.2.23.50:32957 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:299

AP Seq: 0x9F0EAFCF Ack: 0x99CB5D57 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.469713 10.2.23.50:32960 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:286

AP Seq: 0x9F3C0BA8 Ack: 0x3CE3B29 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.473131 10.2.23.50:32961 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:274

AP Seq: 0x9EF4D1BA Ack: 0x47C834A7 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.444883 10.2.23.50:32958 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9E6D8AFD Ack: 0xB266CA4D Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.445527 10.2.23.50:32959 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:272

AP Seq: 0x9ECCD299 Ack: 0x11901CD Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

[**] [1:12592:3] SMTP ClamAV recipient command injection attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

11/11-09:56:34.518056 10.2.23.50:32962 -> 7.204.241.161:25

TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:273

AP Seq: 0x9F11E0AB Ack: 0xC37AAFA4 Win: 0x418 TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-4560][Xref =>http://www.securityfocus.com/bid/25439]

APPENDIX D: NIDP SYSTEM RULE AGAINST INVISIBLE ATTACKS

Following is a rule which can be used by network administrators to detect and prevent their organizations network against invisible attack.

```
Alert tcp any any -> $HOME_NET any (content:"Filetype"; msg: "Our Organization is infected with a risk of invisible attack"; threshold: type limit, track by_src, count 1, seconds 120; classtype: policy-violation; sid: 7000002;)
```

APPENDIX E: LIST OF AUTHOR'S PUBLICATIONS

Paper publish in a book:

- Munir R., Alhomoud A., Awan I, Disso J., "On the Performance Evaluation of Intrusion Detection Systems", Advances in Security Information Management: Perceptions and Outcomes, ISBN: 978-1-62417-204-5, pp. 117-138. 2013.

Papers published in refereed Conferences:

- Alhomoud A., Munir R., Disso J., Awan I., "Performance Evaluation Study of Intrusion Detection Systems", Proc. in 2nd International Conference on Ambient Systems, Networks and Technologies Volume 5, ISSN 1877-0509, 10.1016/j.procs.2011.07.024. Pages 173-180,2011.
- Munir R., Alhomoud A., Disso J., Awan I., "A Performance Evaluation of Intrusion Detection System", Proc. in 27thAnnual UK Performance Engineering Workshop (UKPEW), ISBN 978-0-9559703-3-7, Pages 326-338, 2011.
- Munir R., Disso J., Awan I., Mufti R., "Quantitative Enterprise Network Security Risk Assessment", Proc. in 29th Annual UK Performance Engineering Workshop (UKPEW) 2013.
- Munir R., Disso J., Awan I., Mufti R., "A Quantitative Measure of the Security Risk Level of Enterprise Networks", Proc. in 8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), IEEE, Pages 437-442, 2013.