

AN ANALYSIS OF COMPUTER FORENSIC ACTIVITIES IN DATA NETWORK

BY

LIZ MUTHONI MICHUKI

DCS/17201/72/DF

AND

OLOWO CHARLES OBADI

DCS/17277/72/DU

**RESEARCH REPORT SUBMITTED TO THE SCHOOL OF COMPUTER
STUDIES IN PARTIAL FULFILLMENT FOR THE REQUIREMENTS
OF THE AWARD OF A DIPLOMA OF COMPUTER
SCIENCE OF KAMPALA INTERNATIONAL
UNIVERSITY**

JUNE, 2010

DECLARATION

LIZ MUTHONI MICHUKI and OLOWO CHARLES OBADI do declare that to the best of our knowledge and ability this project report is our own and our original work and has never been presented to any institution for any academic award.

LIZ MUTHONI MICHUKI

DCS/17201/72/DF

Signature: 

Date: 1/07/10

OLOWO CHARLES OBADI

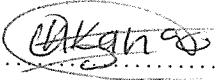
DCS/17277/72/DU

Signature: 

Date: 1/07/10

SUPERVISOR APPROVAL

This project report entitled **an analysis of computer forensic activities in data network** was conducted and written under my supervision.

Signature: 

Date: 01/07/2010

Ms. ONKANGI

DEDICATION

We dedicate this work to our parents, brothers, sisters and colleagues for their moral, material support and encouragement that they have given us during this period.

ACKNOWLEDGEMENT

Heartfelt gratitude to the God almighty for giving as the grace, knowledge and wisdom to have come to this point of Academics. We recognize the guardians namely Mr. and Mrs. Michuki and Mr. and Mrs. Okongo for having given as their encouragement, financial and moral support. Appreciation to Ms Onkangi Caroline our supervisor for her overseeing the project and helping to shape it. Our classmates cannot go unmentioned for their encouragement and support in this project. I would like to honor Mr. Francis Githinji Michuki. words cannot express how much he has inspired our work.

LIST OF ACRONYMS

| | |
|------|--|
| CF | : Computer Forensic |
| NS | : Network System |
| CL | : Courts of Law |
| IT | : Information Technology |
| NIST | : National Institute of Standards and Technology |
| CFTT | : Computer Forensic Tool Testing |
| WGA | : whole genome amplification |
| DOD | : department of defense |
| DDOS | : distributed denial of service attacks |
| SPSS | : statistical package for social study |
| IDS | : intrusion detection systems |
| ISPs | : internet service providers |
| IP | : internet protocol |
| UDP | : user datagram protocol |
| SQL | : structured query language |

LIST OF FIGURES

| | |
|--|----|
| Figure 1: Computer forensic Triage process model..... | 25 |
| Figure 2: General Attack Classification..... | 28 |
| Figure 3: Reaction time as a function of the scanning rate necessary to detect infected hosts and distribute this information Internet-wide. Each curve corresponds to the percentage of infected hosts out of all Vulnerable hosts within 24 hours..... | 30 |
| Figure 4: Containment effectiveness as a function of the deployment scenario Code Red v.2 worm simulation with 100 scans/sec scanning rate..... | 31 |

ABSTRACT

The report summarizes that in this Information Technology age, the needs of law enforcement are changing. Some traditional crimes, especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. According to the website [www.cyber crime.com](http://www.cybercrime.com), an attack is defined as any kind of malicious activity targetted against computer system resources, including, but not limited to, a break-in (any unathourised access), virus infestation, data or destruction, or distributed denial of service attacks.

In addition, some suggest attackers are likely to strike in the midst of confusion that people expect with the arrival of the Year 2000 computer problem. Tribe and Trinoo also may be more powerful than previous programs of the same kind. The duo, which started appearing in recent months, are steps above what has happened before, according to Dave Dittrich, a computer security technician at the University of Washington who wrote analyses of the programs. When installed onto hundreds or thousands of computers, the programs simultaneously bombard a select point on the Internet. If the information from the attackers comes fast enough, the target computer freezes up. Flooding attacks such as Tribe and Trinoo are examples of so-called denial-of-service attacks, a method that's been around as long as there have been networks to inundate.

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. A capability is required to ensure that forensic software tools consistently produce accurate and objective test results. Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing. The researcher used interview, questionnaire, observation and internet and reading materials in order to analyze, collect, and to gather evidence of criminal activity which is admissible in a court of law

TABLE OF CONTENT

| | |
|--|----------|
| DECLARATION..... | i |
| SUPERVISOR APPROVAL..... | ii |
| DEDICATION..... | iii |
| ACKKNOELEDGEMENT..... | iv |
| LIST OF ACRONYMS..... | v |
| LIST OF FIGURES..... | vi |
| ABSTRACT..... | vii |
| CHAPTER ONE..... | 1 |
| 1.0 General Introduction..... | 1 |
| 1.1Background of the study..... | 1 |
| 1.2 Statement of the Problem..... | 3 |
| 1.3 The Project objective..... | 3 |
| 1.3.1 Specific Objective..... | 3 |
| 1.4 Research Questions..... | 4 |
| 1.5 Scope of the study..... | 4 |
| 1.6 Purpose of the study..... | 4 |
| 1.7 Significance of the study..... | 4 |
| CHAPTER TWO..... | 5 |
| LITERATURE REVIEW..... | 5 |
| 2.0 Introduction..... | 5 |
| 2.1Computer Forensics..... | 6 |
| 2.1.2 Examples of Computer Forensics..... | 6 |
| 2.2 Computer Forensics in Law Enforcement..... | 6 |
| 2.2.1 Computer Forensics Certifications..... | 7 |
| 2.2.2 Information technology audit..... | 7 |
| 2.3 Information forensics..... | 8 |
| 2.3.1 Computer forensics tools..... | 9 |
| 2.3.1 Encryption..... | 10 |

| | |
|--|-----------|
| 2.3.2 Public encryption..... | 11 |
| 2.4 Authentication..... | 11 |
| 2.4.1 Computer Attacks..... | 12 |
| 2.4.2 Sources of attacks..... | 13 |
| 2.5 Computer virus..... | 13 |
| 2.5.1 Computer Data Network..... | 14 |
| 2.5.2 computer crimes..... | 14 |
| 2.6 Types of crimes..... | 15 |
| 2.6.1 Digital Evidence..... | 15 |
| 2.6.2 types of evidence..... | 15 |
| 2.7 Typical aspects of a computer forensics investigation..... | 17 |
| 2.7.1 An information system..... | 18 |
| 2.7.2 Components of a system..... | 18 |
| CHAPTER THREE..... | 19 |
| METHODOLOGY..... | 19 |
| 3.0 Introduction..... | 19 |
| 3.1 Research Design..... | 19 |
| 3.2 Study Population..... | 19 |
| 3.3 Sampling design..... | 19 |
| 3.3.1 Sample Size..... | 19 |
| 3.4 Data Collection techniques | |
| 3.4.1 Questionnaire..... | 20 |
| 3.4.2 Observation..... | 20 |

3.4.3 Interview.....20

3.4.4 Internet and reading available Documents.....20

3.5 Data Analysis Methods.....21

CHAPTER FOUR.....22

COMPUTER FORENSICS.....22

4.0 Introduction.....22

4.1 The various computer crimes and attacks.....22

4.3 Theft.....22

4.3 Fraud.....23

4.3.1 Copyright infringement.....23

4.3.2 Cyber Crime (Illegal Exploration and Hacking).....23

4.3.3 Computer Espionage.....24

4.4 The various computer forensic activities.....24

4.5 Different approaches of how a computer system was compromised.....26

4.5.1 Considerations Surrounding the Study of Protection.....26

4.5.2 Technical Underpinnings.....27

4.5.3 General attack classifications.....28

4.5.4 Filters deployment.....28

4.6 Egress filtering.....31

4.7 Honey pots.....31

CHAPTER FIVE.....33

DISCUSSION, RECOMMENDATION AND CONCLUSION.....33

5.0 Introduction.....33

5.1 Recommendation.....33

5.2 Conclusion.....34

REFERENCES.....35

APPENDICES.....36

| | |
|----------------------------------|----|
| Appendix A: Time frame work..... | 36 |
| Appendix B: Budget..... | 37 |

CHAPTER ONE

INTRODUCTION

1.0 General Introduction

The world is becoming a smaller place in which to live and work. A technological revolution in communications and information exchange has taken place within business, industry, and our homes. America is substantially more invested in information processing and management than manufacturing goods, and this has affected the professional and personal lives. The users can bank and transfer money electronically, and many e-mails are received more than letters. It is estimated that the worldwide Internet population is 349 million.

In this Information Technology age, the needs of law enforcement are changing as well. Some traditional crimes, especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. Crimes of violence also are not immune to the effects of the information age. A serious and costly terrorist act could come from the Internet instead of a truck bomb. The diary of a serial killer may be recorded on a floppy disk or hard disk drive rather than on paper in a notebook.

Just as the workforce has gradually converted from manufacturing goods to processing information, criminal activity has, to a large extent, also converted from a physical dimension, in which evidence and investigations are described in tangible terms, to a cyber dimension, in which evidence exists only electronically, and investigations are conducted online.

1.1 Background of the study

Computer forensic science is largely a response to a demand for service from the law enforcement community.

As early as (1984), the federal bureau of investigation Laboratory and other law enforcement agencies began developing programs to examine computer evidence. Currently the company is

using delays to process the required information in an urgent time. Therefore, the main focus for the researcher is to analyze the computer forensic system and to come up with a new system. Therefore the researcher will aim at analyzing the computer forensic activities in a data network in order to gather evidence of criminal activity that can be admissible in a court of law.

An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence. These resources were often scattered throughout the agency. Today, there appears to be a trend toward moving these examinations to a laboratory environment. In (1995), a survey conducted by the United States Secret Service indicated that 48 percent of the agencies had computer forensic laboratories and that 68 percent of the computer evidence seized was forwarded to the experts in those laboratories. As encouraging as these statistics are for a controlled programmatic response to computer forensic needs, the same survey reported that 70 percent of these same law enforcement agencies were doing the work without a written procedures manual Noblett (1995).

There are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations. As early as (1991), a group of six international law enforcement agencies met with several United states federal law enforcement agencies in Charleston, South Carolina, to discuss computer forensic science and the need for a standardized approach to examinations. In (1993), the federal bureau of investigation hosted an International Law Enforcement Conference on Computer Evidence that was attended by 70 representatives of various United States federal, state, and local law enforcement agencies and international law enforcement agencies. All agreed that standards for computer forensic science were lacking and needed. This conference again convened in Baltimore, Maryland,

In (1995), Australia in (1996), and the Netherlands in (1997), and ultimately resulted in the formation of the International Organization on Computer Evidence. In addition, a Scientific Working Group on Digital Evidence was formed to address these same issues among federal law enforcement agencies.

1.2 Statement of the Problem

An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence. These resources were often scattered throughout the agency. In this Information Technology age, the needs of law enforcement are changing as well. Some traditional crimes, especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. The researcher therefore aims at collecting evidence of an attack from a computer system, how the attacker penetrated the system, deduce what was done and gather evidence of criminal activity that can be admissible in a court of law.

1.3 Project objective

1.3.1 Main objective

To analyze computer forensic activities in data network that collected evidence of an attack from a computer system by deducing their actions, and gather evidence of criminal activities that can be admissible in a court of law

1.3.2 Specific Objective

- i) To investigate various computer crimes that attack the computer system.
- ii) To analyze different approaches on how the computer system was compromised
- iii) To implement the mechanism that will prevent the motivation and intent of the attackers to the computer system.

1.4 Research Questions

- i) What kind of problem occur when the system is attacked?
- ii) What baseline of knowledge is necessary for performing incident response and computer forensics?
- iii) What implementation will provide solutions to avoid an attack to the computer system?

1.5 Scope of the Study

The study was concerned with how to collect evidence of an attack and implement measures that are to be used to avoid future attacks to the computer system. further, the tools that was used to carry out Computer Forensics were analyzed.

1.6 Purpose of the Study

To analyze computer forensic activities in a data network, collect evidence of an attack from a computer system and gain more experience in the field of computer forensic network system

1.7 Significance of the Study

After the implementation, computer forensics was well defined and controlled so as not to leave any doubt as to the integrity of the work.

In addition, the researcher also gained more experience in the field of system analysis.

This study was very important to the university in that its students made references to it and make their study a bit easier.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter describes the analysis of computer forensic in a data network system as viewed by different authors. The aim of this chapter is to gather related information of approaches of collecting evidence of an attack from a computer system. How the attacker penetrated the system, deduce what they were able to do, and gather evidence of criminal activity that can be admissible in a court of law). Related information will mainly be extracted from published Computer Forensic text books, internet, previously published journals and dissertations.

2.1 Computer Forensics

A computer forensics is the analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved. Steve Hailey, (2003)

Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage media. Computer forensics is also known as digital forensics. Stellatos, Gerasimos J. (2008)

Computer Forensics is the preservation, identification, extraction, interpretation, and documentation of computer evidence, to include, legal processes, integrity of evidence, factual reporting of the information found, and ability to provide expert opinion in a court of law or other legal proceeding as to what was found.

Confirming or/and Preventing theft of information and intellectual property through internal examination and monitoring usage with Computer Forensics Investigations, in most cases are conducted in a reactionary situation however to-day more pro-active computer forensic examinations are used for monitoring and in some cases A debriefing process for all Exiting Employees.

Computer forensics has different facets, and is not just one thing or procedure. At a basic level, computer forensics is the analysis of information contained within and created with computer systems, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved. This being said, computer forensic techniques and methodologies are used for conducting computing investigations - again, in the interest of figuring out what happened, when it happened, how it happened, and who was involved.

In many cases, information is gathered during a computer forensics investigation that is not typically available or viewable by the average computer user, such as deleted files and fragments of data that can be found in the space allocated for existing files - known by computer forensic practitioners as slack space. Special skills and tools are needed to obtain this type of information or evidence.

2.1.2 Examples of Computer Forensics

Recovering thousands of deleted emails

Performing investigation post employment termination

Recovering evidence post formatting hard drive

Performing investigation after multiple users had taken over the system

2.2 Computer Forensics in Law Enforcement

A computer forensic in law enforcement is on the premises of a crime scene; the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined (even if very briefly) by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be tainted. If you currently have computer evidence that you have seized as part of an investigation and you are unsure how to proceed, please contact us. We will gladly provide a short consultation at no charge to your department. More in-depth assistance can range from consultation to hands-on help with all steps of the process. If you anticipate seizing a computer or computer evidence, and do not have the services of a computer forensics specialist, we can provide valuable advice and

help on all steps of the process: affidavit and warrant preparation, search and seizure, analysis and court presentation.

The Support to Law Enforcement Berry hill (2002) Computer Forensics provided extensive support to law enforcement agencies at the municipal, state and federal levels. Case types have included credit card theft, tax fraud, immigration fraud, arson, homicide, child pornography and others. The background in law enforcement combined with our expertise in computer forensics makes us the perfect solution for your computer evidence problems.

2.2.1 Computer Forensics Certifications

The rate of fraud, abuse and downright criminal activity on IT systems by hackers, contractors and even employees are reaching alarming rates. Corporate IT, Law Enforcement and Information Security Pros are often required to perform computer forensics duties on their jobs. In terms of job growth, nothing beats computer forensics as a career, and no one can beat InfoSec Institute as the best place to learn from a computer forensics training expert. John Lister (2010)

2.2.2 Information technology audit

An information technology audit is an examination of the checks and balances, or controls, within an information technology (IT) group. An IT audit collects and evaluates evidence of an organization's information systems, practices, and operations. The evaluation of this evidence determines if the information systems are safeguarding the information assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's business goals or objectives. The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

The organization's computer systems are available for the business at all times when required?
(Known as availability)

The information in the systems is disclosed only to authorize users? (Known as security and confidentiality)

The information provided by the system always is accurate, reliable, and timely? Further more, the fundamental requirement for effective auditing is to provide an opinion to the executive team and the board audit committee on the adequacy of the internal control framework operating within the organization's information technology and telecommunications (IT&T) environment. This requirement, while ongoing, may have specific meaning at some point, e.g., financial year-end when management is required to sign off on the end of year accounts.

IT auditors have used a range of audit methodologies and techniques to support their audit opinions. This paper will outline an approach recently utilized within a financial services organization to provide an annual assessment of the IT&T internal control framework. The approach used is based on a set of internationally recognized IT service delivery and support process models called ITIL (Information Technology Infrastructure Library) and rely extensively on the use of control self-assurance (CSA) workshops facilitated by IT audit staff. This approach can be applied with equal success to internal and outsourced IT&T environments.

CSA is a risk management program where risks and controls are examined and assessed to provide reasonable assurance to management that business objectives will be met. IT management and staff involved in the delivery of services and products to an organization participate in all phases of the process. For CSA to be effective it must have support from IT&T management and staff.

2.3 Information forensics

Information forensic investigation dwells into the aspects of creation, operation and evolution of the enterprise information system. Specifically, investigation focuses on causal factors and processes that govern the life cycle implementation of such systems. Forensic investigation may be initiated when a system is suspect or compromised; generally, investigation occurs when a system fails. Investigations normally concentrate on specific problem areas or components of a system; the intricacies of business systems, costs and resources available, often preclude detailed examination of the whole information system. Nevertheless, bringing about scientific

examination of facts when problems occur is not only prudent, but necessary for the court of law. The methodological approach to investigation at present is the subject of research interest and topical development.

The IEEE Transactions on Information Forensics and Security covers the sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features. Information Forensics is the science of investigation into systemic processes that produce information. Systemic processes utilize primarily computing and communication technologies to capture, treat, store and transmit data. Manual processes complement technology systems at every stage of system processes; e.g. from data entry to verification of computations, and management of communications to backing-up information reports. In context, both technology and manual systems, with systemic processes that are either proprietary by design or evolved inconsequentially, constitute the enterprise Information System. The complexity of enterprise business systems, in particular those augmented with technology and legacy systems, often are susceptible to fraud, abuse, mistakes, and sabotage.

2.3 Computer forensics tools

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. A capability is required to ensure that forensic software tools consistently produce accurate and objective test results. Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing.

2.3.1 Encryption

Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the scrambling of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearranges the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key. Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher that is, the harder it is for unauthorized people to break it the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could

hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption. Doga Ulas Eralp, (2002)

2.3.2 Public encryption

Cryptographic system that uses two keys a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. Public-key systems, such as pretty good privacy, are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. What's needed, therefore, is a global registry of public keys, which is one of the promises of the new LDAP technology.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called Diffie-Hellman encryption. It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption).

2.4 Authentications

Over the past twenty years, DNA analysis has revolutionized forensic science, and has become a dominant tool in law enforcement. Today, DNA evidence is key to the conviction or exoneration of suspects of various types of crime, from theft to rape and murder. However, the disturbing possibility that DNA evidence can be faked has been overlooked. It turns out that standard molecular biology techniques such as, molecular cloning, and recently developed whole genome amplification (WGA); enable anyone with basic equipment and know-how to produce practically unlimited amounts of in vitro synthesized (artificial) DNA with any desired genetic profile. This artificial DNA can then be applied to surfaces of objects or incorporated into genuine human

tissues and planted in crime scenes. Here we show that the current forensic procedure fails to distinguish between such samples of blood, saliva, and touched surfaces with artificial DNA, and corresponding samples with in vivo generated (natural) DNA. Furthermore, genotyping of both artificial and natural samples with Profiler Plus yielded full profiles with no anomalies. In order to effectively deal with this problem, we developed an authentication assay, which distinguishes between natural and artificial DNA based on methylation analysis of a set of genomic loci: in natural DNA, some loci are methylated and others are unmethylated, while in artificial DNA all loci are unmethylated. The assay was tested on natural and artificial samples of blood, saliva, and touched surfaces, with complete success. Adopting an authentication assay for casework samples as part of the forensic procedure is necessary for maintaining the high credibility of DNA evidence in the judiciary system.

2.4.1 Computer Attacks

According to the website www.cybercrime.com, an attack is defined as any kind of malicious activity targetted against computer system resources, including, but not limited to, a break-in (any unauthorised access), virus infestation, data or destruction, or distributed denial of service attacks.

In addition, some suggest attackers are likely to strike in the midst of confusion that people expect with the arrival of the Year 2000 computer problem. Tribe and Trinoo also may be more powerful than previous programs of the same kind. The duo, which started appearing in recent months, are steps above what has happened before, according to Dave Dittrich, a computer security technician at the University of Washington who wrote analyses of the programs.

When installed onto hundreds or thousands of computers, the programs simultaneously bombard a select point on the Internet. If the information from the attackers comes fast enough, the target computer freezes up.

Flooding attacks such as Tribe and Trinoo are examples of so-called denial-of-service attacks, a method that's been around as long as there have been networks to inundate. And launching attacks from several computers too has been tried before, for example with the attacks of last year.

But Tribe and Trinoo give a new level of control to the attacker, and they are being improved, Dittrich said.

2.4.2 Sources of attacks

Chertoff noted that by comparison, physical attacks are relatively easy to track down and respond to. In the Cold War we could attribute an attack. It was clear where it came from and we could respond, he said.

Finding the source of cyber attacks, though, is far more complicated, he said. While investigators could find the physical systems from which an attack is launched, the owner of the systems could have nothing to do with the criminal activity. The difficult task of identifying the true sources of cyber attacks remains one of the biggest challenges in the development of a national cyber security strategy, former Department of Homeland Security Secretary Michael Chertoff told Computerworld in an interview at the RSA Security conference here today. Chertoff, who is participating in a panel discussion at the conference, said there is a growing need for the U.S to create a strong, formal strategy for responding to cyber attacks against American interests.

Such a strategy would need to clearly articulate possible U.S. responses to attacks, which could include diplomatic and other tools.

2.5 Computer virus

A computer virus is a computer program that can copy itself and infect a computer. The term virus is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

Malware includes computer viruses, worms, trojans, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software, including true viruses. Viruses are sometimes confused with computer worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan is a program that appears harmless but hides malicious functions. Worms and Trojans, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious and go unnoticed.

2.5.1 Computer Data Network

Data network is a collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with other users. Networks may be classified according to a wide variety of characteristics. This article provides a general overview of types and categories and also presents the basic components of a network.

2.5.2 computer crimes

There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate. Nevertheless, there is a consensus among both law enforcement personnel and computer scientists who specialize in security that both the number of computer crime incidents and the sophistication of computer criminals are increasing rapidly. Estimates are that computer crime costs victims in the USA at least US\$ 5×10^8 /year and the true value of such crime might be substantially higher. Experts in computer security, who are not attorneys, speak of information warfare. While such information warfare is just another name for computer crime, the word warfare does fairly denote the amount of damage inflicted on society.

2.6 Types of crimes

Property crimes were committed more frequently (one every 3.0 seconds) than violent crimes (one every 22.1 seconds), down from one every 19 seconds in 1996. The Crime Clock does not imply these crimes were committed with regularity; instead it represents the relative frequency of

occurrence. Note this frequency of occurrence does not take into account population increases, as does the per capita crime rate.

The FBI, in its annual Crime in the United States report, publishes data for serious crimes in the Crime Index. The Index includes murder, rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson.

Although the number of crimes in the United States in 2002 remained high, at over 11.8 million, the total of Crime Index offenses remained relatively unchanged from 2001, rising only by 0.1 percent. Violent crimes comprised 12.0 percent of all Crime Index offenses in 2002, while property crimes accounted for 88.0 percent. The Crime Index rate, which equals the number of Crime Index offenses per 100,000 inhabitants, actually registered a 10.9 percent drop from the 1998 rate.

2.6.1 Digital Evidence

According to www.htcia.org, Evidence is defined as any physical or electronic information (such as written or electronic documentation, computer log files, data, reports, physical hardware, software, disk images, etc) collected during a computer forensics investigation. Evidence includes, but is not limited to, computer-generated files (such as log files or generated reports) and human-generated files (such as spreadsheets, documents, or email messages).

The purpose of gathering evidence is to help determine the source of the attack, recover from any damage resulting from the attack, and to introduce the evidence as testimony in a court of law during a prosecution, the evidence must be admissible in court and be able to withstand challenges as to its authenticity.

2.6.2 Types of evidence

2.6.2.1 Anecdotal Evidence

Usually very weak positive evidence; Description of one, or a small number of specific instances, presumably of the same type, general nature, or structure. Better used as 'negative' evidence; as counter examples

An anecdote is one sort of example. How does anecdotal evidence really work? Obviously an anecdote, or another kind of example, cannot prove a general statement, so avoid treating a single case as proving a general point. On the other hand, a single anecdote or counter example is alone sufficient to disprove a general statement. One successful anecdote will show that one must modify one's claim. An anecdote will not count as weighty evidence, however, either in support of or in opposition to a more limited, narrower claim, which is not intended to apply generally.

2.6.2.2 Testimonial Evidence

1. Moderately strong or supportive evidence
2. Reference to an established or trustworthy authority

For a philosophy paper, one must (generally) use well-established or credible sources. The testimony of credible persons will sometimes strengthen an argument, but one must almost always say why the reader should especially consider that person's comments. Give credentials. Don't assume, however, that respectable credentials alone establish the fact that we should accept the testimony without question. You should know when experts disagree on an issue, so that one expert's assessment does not alone establish the point. Popular magazines with light reading fare such as *Cosmopolitan* and *People* seldom, if ever provide anything which would strengthen an argument in a philosophy paper. Always give your own comment on a quote or reported view. Don't just report what the authority claims; say why the reader should seriously consider it, and demonstrate your own understanding of it.

2.6.2.3 Statistical Evidence

1. Moderately strong or supportive evidence
2. Reference to empirical analysis, or to the results of methodical or scientific experiments or investigations.

When you structure part of your argument using statistics, always report the source. Since statistics from different sources may vary or conflict, give reports from multiple sources when possible. Whenever possible, as you report your source, show that it is a reputable one.

Analogical Evidence

1. Fairly strong or supportive evidence (of a sort)
2. Explanatory modeling of the target phenomenon by means of a comparison with an already understood, or more easily understood, phenomenon

Analogies provide interest and hopefully illumination to a line of argument. However, you must be cautious when you create your own analogy or evaluate someone else's. The logical power of an analogy is often overestimated. Usually an analogy will help a person understand a relation and see new connections between things, but seldom does it provide hard proof of a conclusion or thesis for a person who ardently resists that view. Analogies are especially useful for articulating a new perspective that has just been supported by empirical evidence, because they often illustrate rather than establish points of view.

2.7 Typical aspects of a computer forensics investigation

To investigate computers as an investigator it is important to understand the kind of potential evidence they are looking for in order to structure their search. Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. Second, the investigator must pick the appropriate tools to use. Files may have been deleted, damaged, or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process.

The two basic types of data are collected in computer forensics. Persistent data is the data that is stored on a local hard drive and is preserved when the computer is turned off. Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory. Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it.

System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that is critical to the identification and analysis of a security incident.

2.7.1 An information system

A system is a group of interrelated components working together towards a common goal by accepting inputs and producing outputs in an organized transformation process (O'Brien, 2000, pg 8).

It is technically as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making, coordination, and control in an organization. In addition to supporting decision making, coordination, and control, information systems may also help managers and workers analyze problems, visualize complex subjects, and create new products (O'Brien, 1997, Pg 7)

2.7.2 Components of a system

Input; It involves capturing and assembling elements that enter the system to be processed. For example, raw materials data and human effort must be secured and organized for processing.

Processing; It involves transformation processes that convert input into output. For example, it can be manufacturing process or mathematical calculations.

Output; It involves transferring elements that have been produced by a transformation process to their ultimate destination. For example, finished products, human services, and management information must be transmitted to their human users (O'Brien, 2000, p 8).

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter provides a general overview of the data gathering method used to collect data for analyzing computer forensic activity.

3.1 Research Design

This study was both descriptive and analytical survey in nature. This study elaborated the different views on analyzing computer forensic data network. A survey design was employed because the researcher got views of respondents about the study. This research design was useful because the researcher intends to find out the problems of computer forensic data network.

3.2 Study Population

The study took place with the Computer forensic scientists who are largely a response to a demand for service from the law enforcement community.

3.3 Sampling design

Simple random sampling method was used to select a sample from the population. Non probability sampling design, where all members from a study population had equal chances of being selected as respondents

3.3.1 Sample Size

The study involved a purposive sampling research data collection. The first stage involved the selected population of the study. Secondly the researcher identified potential respondents that included, share holders and executive managers. From each enterprise two respondents was selected to constitute a sample size to 60 respondents.

3.4 Data Collection Techniques

3.4.1 Questionnaire

Using this method, a researcher used as a printed document to the company which contained standardized questions that were to be answered by the users of the current system and to some of the staff, to gather evidence of criminal activity was admissible in a court of law.

The methods was used because, it enabled the respondents to answer the questions in their free time and it gave an opportunity to get accurate information since it was designed in less tense environment .

3.4.2 Observation

Using this method, the researcher had to observe important points that was not revealed by the respondents in interview on analysing the computer forensic system. This method was re-approved the validity of the data collected through interview that could not provide a clear explanation by the respondents.

3.4.3 Interview

With this method, the researcher visited the company offices. This provided the researcher with information regarding how the system performs and the attacks. From this the researcher was able to analyze the system.

3.4.4 Internet and reading available Documents

The growing popularity of the Internet has brought a major shift in Electronic Data Reporting and data collection. The researcher took the advantage of the internet being an ocean of information to study well established organization that uses the federal bureau of investigation Laboratory and other law enforcement agencies began developing programs to examine computer attack.

The researcher also accessed some enforcement of laws and look at how they are issued which helped in designing of the proposed system and redesigning the forms to suit the computerized applicant's database environment law enforcement systems.

3.5 Data Analysis

Data collected from different methods used was compared which gave the researcher a clear understanding of the problem. Data was sorted to get a clear picture of what would be the inputs and the expected outputs and reports. The researcher analyzed the data using SPSS programme.

CHAPTER FOUR

COMPUTER FORENSICS

4.0 Introduction

This chapter provides an overview of the various types of crimes and attacks that occur in a computer system.

4.1 The various computer crimes and attacks

With the popularization of the Internet, interest in computer crime, ethics, and privacy has gained momentum. News items describe identity theft, credit card numbers posted on chat rooms, and child pornography web sites. For example, in July, 2001, according to MSNBC.com reporter Bob Sullivan reported that key personal data including Social Security numbers, date of birth, driver's license numbers, and credit card information was posted up in a chat room. Investigations have yet to reveal the extent or perpetrators. However, affected individuals have already experienced fraudulent financial transactions on personal accounts the rich and famous are not exempt from such experiences. Bill Gates, Steven Spielberg, and Oprah Winfrey are among the notables who have experienced identity theft.

Information systems vulnerabilities cover more territory than just personal losses. Computer information systems are vulnerable to physical attacks, electronic hacking, and natural disasters. With computer information systems serving as the vital life blood of many organizations, managers must be aware of both the risks and the opportunities to minimize the risks to information systems.

4.2 Theft

Theft in computer crime may refer to either unauthorized removal of physical items such as hardware or unauthorized removal or copying of data or information. It is well known that laptop computers are targeted at airports and restaurants. The prize garnered with theft of a laptop is usually the data or information such as passwords for corporate systems contained on the laptops rather than the hardware.

4.3 Fraud

Fraud on the Internet may run the gamut from credit card offers which are utilized only to capture personal information, to investor postings which promote a stock or investment offer to encourage investment which will benefit the person posting the information, to medical and pharmaceutical related sites which provide correct medical advice or sell altered medications.

4.3.1 Copyright infringement.

The Internet has provided a unique opportunity and environment for copyright infringement. This type of computer crime encompasses use of software, music, etc which is not appropriately acquired (purchased). Software piracy occurs more easily with the ability to post files for downloading all over the world. However, another more costly copyright infringement occurs when trademarks and logos of corporations are posted on non-authorized web sites. Some criminals utilize the trademarks and logos to appear to be a legitimate site to perpetrate fraud. Many corporations have employees or consulting contractors who constantly crawl the web to sniff out illegal usage of trademarks and logos.

Ridge top Information.

4.3.2 Cyber Crime (Illegal Exploration and Hacking)

This computer attack combines several different types of unintentional actors into one category defined as cyber crime or “hacker“. Although this category of hacker includes many kinds of cyber criminals, from a DOD perspective, the motivation of a hacker without intent to damage the national security of the United States is the importance difference. Therefore, it is necessary to differentiate between cyber crime and other levels of computer attack because it will affect the type of DOD response.

Cyber crime in the form of a cyber intrusion (hacking) is illegal access into a network system and can range from simple exploration causing no damage to malicious hackers who are intent on causing loss or damage. Most information systems tend to divide the world into at least three parts: outsiders, users, and super users. A popular route of attack for hackers is first to use a password attack so that the outsider becomes a user, and then once a user, he will use known weaknesses of Unix programs so that he can access super user privileges. Once a super user, a

hacker can read or alter files; control the system; make it easier to re-enter the system (even after tougher security measures are enforced); and insert rogue code (for example a virus, logic bomb, and Trojan horse, for later exploitation. Although the other levels of cyber-attack to include cyber espionage, cyber-terrorism and information warfare also use a similar method of hacking into an internet connected system, the main distinction between a hacker and the other levels is the intention of the perpetrator.

4.3.3 Computer Espionage

This threat is likely to be the most difficult to distinguish because it may appear to be hacker activity and will intentionally avoid causing damage or harm in order to avoid detection. Although there is little information in the public domain about the use of computer hacking in foreign intelligence operations, there is no doubt that this activity is prevalent among most state intelligence agencies around the world. The first documented computer espionage case was in 1986 and was immortalized in the best seller novel, —The Cuckoos Egg“. In this case, the Soviet KGB levied five hackers (to include the Hanover Hacker) to hack into US DOD systems and provide information to the Soviets. These young hackers all had drug and financial problems and were easily exploited by the Soviet KGB. This early espionage investigation revealed the importance of cyber espionage to foreign intelligence services and also the proclivity for criminal hackers to be vetted and employed by foreign intelligence services.

4.4 The various computer forensic activities

Computer Forensics refers to “the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded”. There are many instances of where crimes involving a computer need to be investigated. These crimes range from child exploitation to a network breach resulting in the theft of personal data or the destruction of digital information. In today’s digital world, it is important to put a real person behind the keyboard of any type of cyber event, primarily in instances of cybercrime. Computer Forensics attempts to do exactly that. “The core goals of computer forensics are fairly straightforward: the preservation, identification, extraction, documentation, and interpretation of computer data.” In order to do this, there are generally two types of data that are collected in computer forensics. Persistent data, which is data stored on a local hard drive or another medium.

This type of data is preserved when the computer is powered off. There is also volatile data, which is any data stored in memory, or exists in transit. This refers to data that is lost when the computer loses power or is turned off. This type of data resides in cache and RAM. Depending on the nature of the crime, skill or knowledge the cybercriminal has relating to computers or origin of the cyber event, the digital evidence remaining as proof of the event may be limited. Also, what little evidence that is recovered, or could be recovered, becomes a vital part of the legal proceedings that could follow. Examples of computer forensic activities include; Recovering thousands of deleted emails, Performing investigation post employment termination, Recovering evidence post formatting hard drive, performing investigation after multiple users had taken over the system.

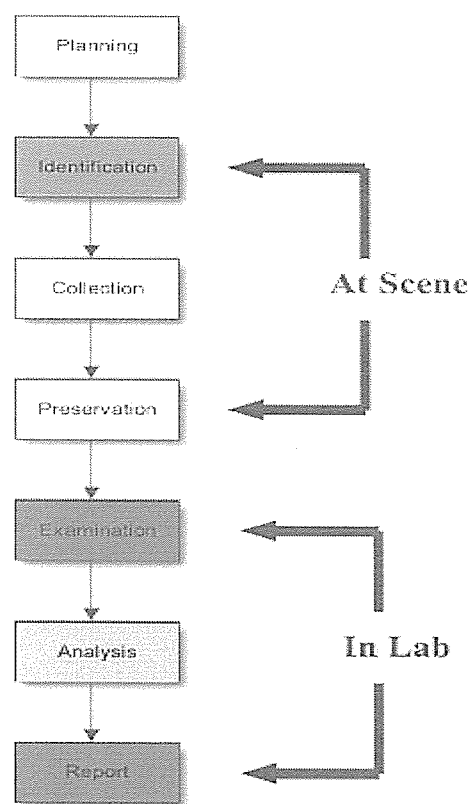


Figure: 1 Computer forensic Triage Process Model

4.5 Different approaches of how a computer system was compromised

The researcher found out the various approaches of how a computer system can be compromised in relation to protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures--whether hardware or software--that are necessary to support information protection.

4.5.1 Considerations Surrounding the Study of Protection

According to the research survey, the major concern is multiple use. For those applications in which all users should not have identical authority, some scheme is needed to ensure that the computer system implements the desired authority structure. For example, in an airline seat reservation system, a reservation agent might have authority to make reservations and to cancel reservations for people whose names he can supply. A flight boarding agent might have the additional authority to print out the list of all passengers who hold reservations on the flights for which he is responsible. The airline might wish to withhold from the reservation agent the authority to print out a list of reservations, so as to be sure that a request for a passenger list from a law enforcement agency is reviewed by the correct level of management. The airline example is one of protection of corporate information for corporate self-protection (or public interest, depending on one's view). A different kind of example is an online warehouse inventory management system that generates reports about the current status of the inventory. These examples span a wide range of needs for organizational and personal privacy. All have in common controlled sharing of information among multiple users. All, therefore, require some plan to ensure that the computer system helps implement the correct authority structure. Of course, in some applications no special provisions in the computer system are necessary. It may be, for instance, that an externally administered code of ethics or a lack of knowledge about computers adequately protects the stored information. Although there are situations in which the computer need provide no aids to ensure protection of information, often it is appropriate to have the computer enforce a desired authority structure. This can be categorized in the following ways;

1) Unauthorized information release: an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to "traffic analysis," in which the intruder observes only the patterns of information use and from those patterns can infer some information content. It also includes unauthorized use of a proprietary program.

2) Unauthorized information modification: an unauthorized person is able to make changes in stored information--a form of sabotage. Note that this kind of violation does not require that the intruder see the information he has changed.

4.5.2 Technical Underpinnings

The researcher found out that it was worth to begin the development of the technical basis of information protection in modern computer systems. There are two ways to approach the subject: from the top down, emphasizing the abstract concepts involved, or from the bottom up, identifying insights by studying example systems. It follows the bottom-up approach, introducing a series of models of systems as they are, built in real life. It then extends these two models to handle the dynamic situation in which authorizations can change under control of the programs running inside the system. Further extensions to the models control the dynamics. The final model (only superficially explored) is of protected objects and protected subsystems, which allow arbitrary modes of sharing that are unanticipated by the system designer. These models are not intended so much to explain the particular systems as they are to explain the underlying concepts of information protection. The main emphasis throughout the development is on direct access to information (for example, using LOAD and STORE instructions) rather than acquiring information indirectly (as when calling a data base management system to request the average value of a set of numbers supposedly not directly accessible). Control of such access is the function of the protected subsystems developed near the end of the paper. Herein lies perhaps the chief defect of the bottom-up approach, since conceptually there seems to be no reason to distinguish direct and indirect access, yet the detailed mechanics are typically quite different.

4.5.3 General attack classification

Recently many prominent web sites face Distributed Denial of Service Attacks (DDoS). While security threats could be faced by a tight security policy and active measures like using firewalls and vendor patches. These DDoS are new in such way that there is no completely satisfying protection yet. In this section we categorize different forms of attacks and give an overview over the most common DDoS tools. Furthermore we present a solution based on Class Based Routing mechanisms in the Linux kernel that will prevent the most severe impacts of DDoS on clusters of web servers with a pretended load balancing server. The goal is to keep the web servers under attack responding to the normal client requests. This can be shown in the diagram below;

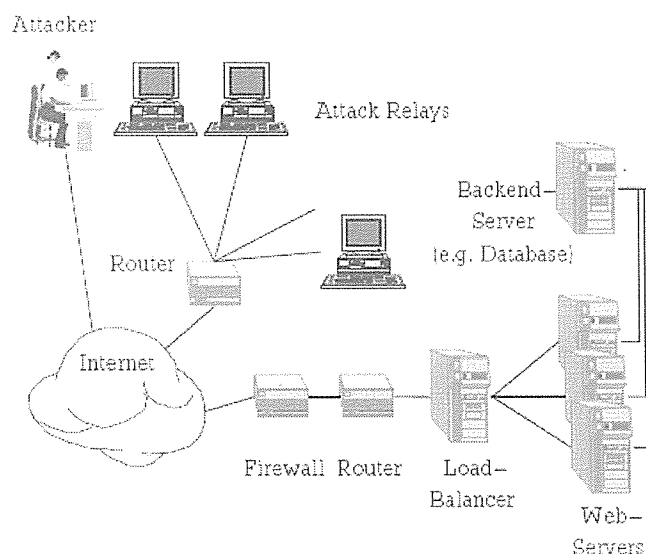


Figure 2: General Attack Classification

4.5.4 Filters deployment

In particular, reaction time up to 10 seconds is sufficient to stop even fastest bandwidth-limited scanning worms. Further analysis shows that it is much easier to deploy the filters at the leading ISPs because almost every customer PC has to participate in the filtering activity otherwise. In practice, however, this task cannot be accomplished on the ISP side because even signature-based Intrusion Detection Systems (IDS) cannot deal with the amount of traffic flowing at that

level. The problem of automatic new worm patterns recognition at that level is not even considered here. The amount of false positives is so enormous that no human is able to process and react to them. The only possibility is to slow suspicious traffic down to allow more reaction time for other worm containment mechanisms. Worm filters are usually state full and thus backbone traffic analysis requires huge amounts of data to be revised with almost any packet processed. IP spoofing and proxies introduce further problems for filters located at ISPs. In addition, the impact of the false detections and cutting off legitimate traffic can be minimized if a smaller portion of the network is being filtered. Another important problem is that multi-vector worms can penetrate most of the filters by using some slower spread means. Alternatively, any mobile user can bring the worm behind any firewall inside of his laptop. Once the high level filter is passed the worm can easily spread inside of the ISP infrastructure. One more reason to deploy filters close to the end hosts are that configuration of filters can be better optimized if the expected traffic patterns.

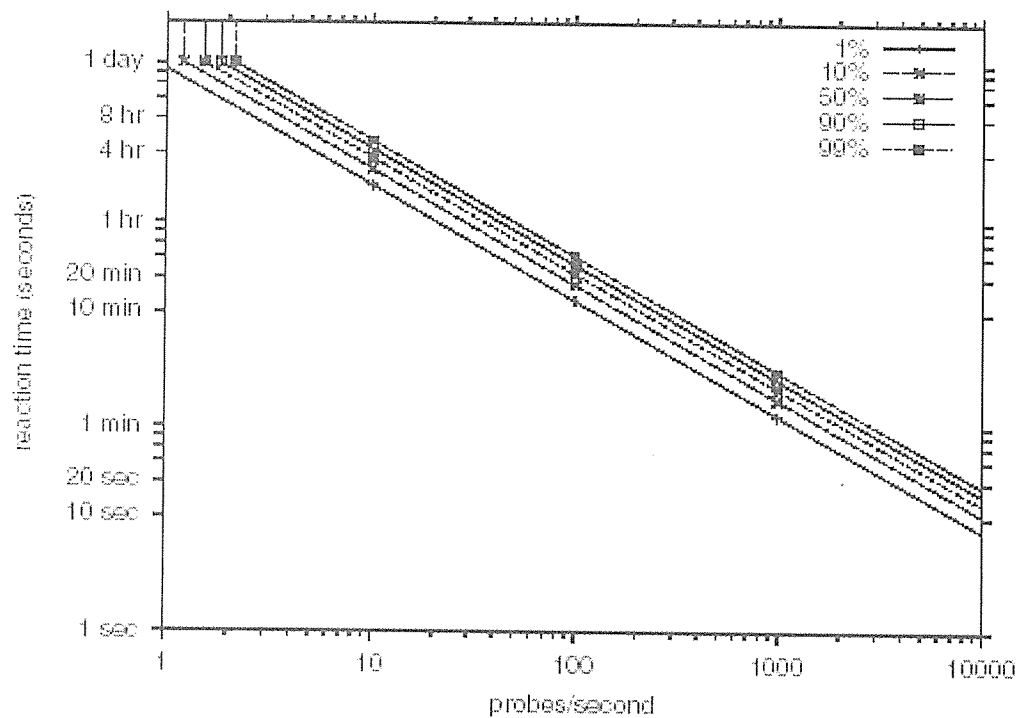


Figure 3: Reaction time as a function of the scanning rate necessary to detect infected hosts and distribute this information Internet-wide. Each curve corresponds to the percentage of infected hosts out of all vulnerable hosts within 24 hours.

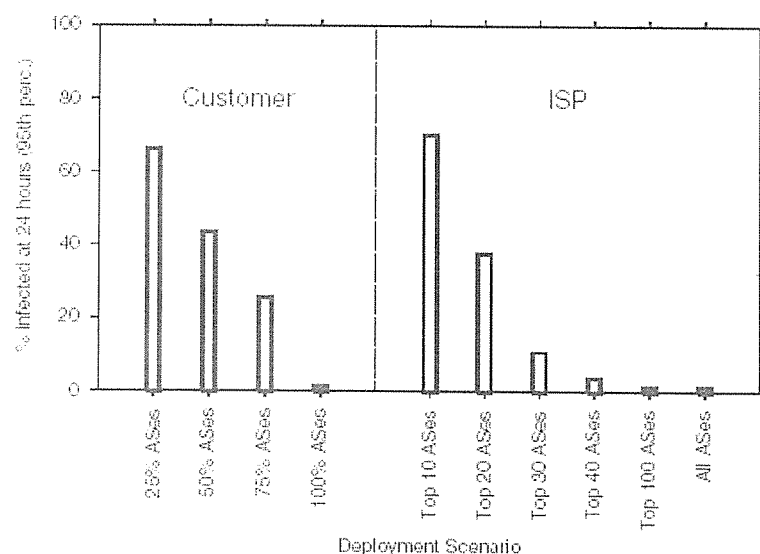


Figure 4: Containment effectiveness as a function of the deployment scenario Code Red v.2 worm simulation with 100 scans/sec scanning rate.

4.6 Egress filtering

The most natural and reliable way to stop all scanning worms is to stop outgoing scanning activity on every host or at least organizational level. Technically this detection process is very simple. If a given host tries to contact too many new hosts it is extremely suspicious. However, as illustrated the example of the spoofed IP address filtering people is not eager to protect others even if there is a minimal risk that some legitimate traffic will be filtered out. A simple solution to this problem is to slow down suspicious traffic instead of blocking it. It is important to understand that this process of filtering is not completely altruistic: Firstly, infected hosts are detected as soon as possible. Secondly, local networks are not flooded with scanning packets.

4.7 Honey pots

A very reliable anti-scanning mechanism can be constructed based on the honey pots. Such an infrastructure can consist of many machines without any production purpose. More importantly these machines do not advertise themselves on the Internet. Therefore, any attempt to access any such honey pot can be only a result of scanning. Once the scanning source is identified the corresponding traffic can be blocked for other machines too. Honey pots are generally divided into low-interaction honey pots and high interaction honey pots. Low-interaction honey pots generally monitor unused IP space or provide simple fake resources. High-interaction honey pots

are usually real systems running real software. They allow gaining more information about hackers' activity and tactics. There are a number of problems related to the honey pot applications. Most importantly, it is not quite clear if the honey pots usage is legal. Another inherent problem of any honey pot is that this simple approach opens an easy way to create denial of service attacks if the scanning traffic patterns are spoofed. Unfortunately, there are many ways for worms to avoid detection by honey pots by spoofing packet source addresses as in the case with single packet UDP worm like SQL Slammer or distributed scanning networks like Stumbler. Correct honey pot implementation is another issue. Honey pots have to process too many scanning packets at the peak of the worm epidemics and may not sustain it. High interaction honey pots may become subverted and used by worms if implemented wrong roll, the honey pot approach is very promising because it can even stop flash.

CHAPTER FIVE

DISCUSSION, RECOMMENDATIONS AND CONCLUSION

5.0 Introduction

This chapter deals with the conclusion of the findings and the recommendations of the project.

5.1 Discussion

The findings on computer forensic activities in data network in relation to the various computer crimes and mechanisms put in place to protect computers, and gather evidence of criminal activities that can be admissible in a court of law, the findings according to the researcher began with various computer crimes that attack the computer system, the various computer forensic activities, different approaches of how the computer system was compromised and the mechanisms that will prevent the motivation and intent of the attackers to the different computer systems. The study faced a lot of limitations that retarded the smooth running of the study to be finished in the required time. These are;

Some of the staff members to be interviewed were absent, which delayed the researcher to move to the next stage of the project.

It may make the project costly in terms of finance, accrued from transport.

There may be lack of materials such as computers, secondary storage devices such as floppy, flush disk, etc to use during the study.

It was difficult to convince some of the staff members about the needs of developing a new system since most of them had no knowledge about the use of computers in criminal enforcement in a court of law.

As the researcher went ahead with the study, the researcher may realize that there is no success with all the above shortcomings. So, the researcher will do the following to overcome them;

A researcher will befriend the users of the system in order to give out the required information.

A researcher was advised from the supervisor who guided and direct on how to overcome some problems.

5.2 Recommendations

Despite the fact that general methods like software diversification and compile/run-time protection should be effective against many stealth worms, their use requires deployment on every host and thus is complicated by the social/administrative reasons. Fortunately, relatively slow spread of topological worms makes it possible to counter them using signature-based detection methods. So far security experts pushed by the competitive antiviral market demands demonstrated that a slow spreading worm-like threat could be identified and confirmed by humans within one day while some signatures can be created even before the worm outbreaks. This gives a chance that topological worms can be filtered out by the signature-based filters before such worms are widely spread especially if the signatures are distributed in the fast and automatic way. As well as any other conclusion this one has some exceptions. Thus, P2P networks have a very high degree of connectivity and the process of creation of many new connections has to be considered normal.

5.3 Conclusion

Law enforcement agencies face many challenges in responding to information attacks in cyber space particularly attacks that cross national and regional borders and exploit technologies of concealment. It can be difficult to locate a hacker who has looped through multiple systems, used anonymous services, or entered through a wireless connection from a mobile unit. Another challenge is collection and preservation of evidence. Evidence may be encrypted or dispersed across several countries. Tracking an intruder who has used a computer located in the United States will require searches and seizures or wiretaps.

REFERENCES

- Adelman, C. (2000), *the Certification System in Information Technology*. Washington: US Department of Education
- Anderson, D. (2000), *managing information systems*. Codd, F. (1970), *A relational model of data for large shared data Banks*. 13 (6): Pp377–387
- Darwen, H. (2000), *Foundation for Future*. www.management-hub.com.
- D. Andersen, "Mayday: *Distributed Filtering for Internet Services*," 4th USENIX
- Hutchinson, S. and Sawyer, S. (2000). *Computers communications information*. Seventh Edition, pp12.13.
- L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, "On the implications of Zipf's law for web caching," *Technical Report CS-TR-1998-1371*, University of Wisconsin, Madison, Apr. 1998
- McFadden, R and Hoffer, A. (1993), *Modern database management*. Fourth Edition, P30
- O'Brien, J. (2001), *Introduction to information systems*. Tenth Edition.
- Ramakrishnan, G. (2000), *Database management systems*. Second Edition.
- Schultheis, S. (1989), *Management information systems*. Second Edition, pp207.
- Symposium on Internet Technologies and Systems, March 2000
- Vladimir, Z. (1998), *Foundation of information systems*. pp209.
- The Free Network Project, <http://freenet.sourceforge.net/>

APPENDIX A: TIME FRAME WORK

| Project schedule | | | | | | | | | | |
|------------------|---------------------------------|------|-----|-----|-----|-----|------|------|-----|------|
| TASK | | 2009 | | | | | 2010 | | | |
| | | OCT | NOV | DEC | JAN | FEB | MAR | APRI | MAY | JUNE |
| 1 | Feasibility study | | | | | | | | | |
| 2 | Data collection | | | | | | | | | |
| 3 | Data analysis | | | | | | | | | |
| 4 | Proposal writing and acceptance | | | | | | | | | |
| 5 | Report writing and presentation | | | | | | | | | |
| 6 | | | | | | | | | | |

This gaunt chart above shows the plan of how the researcher budgets his time to accomplish a goal.

APPENDIX B: BUDGET

| ITEM | COST |
|---------------------|--------------------|
| Flash Disk | Shs 60,000 |
| Transport | Shs 100,000 |
| Pens | Shs 5000 |
| Internet | Shs 30,000 |
| Typing and Printing | Shs 50,000 |
| Photocopies | Shs 30,000 |
| Miscellaneous | Shs 56,000 |
| Total | Shs.331,000 |