

ETHICAL HACKING AND NETWORK SECURITY TO PREVENT NETWORK CYBER ATTACKS

By

AOBAKWE PEDDIAH ARMANDO

A THESIS

**SUBMITTED TO THE FACULTY OF COMPUTERS
BOTHO UNIVERSITY**

**FOR MASTERS IN COMPUTER SYSTEMS MANAGEMENT
MAY 2019**



Table of Contents

Dedication	3
Acknowledgement	4
Tables	5
Figures	6
Abstract.....	7
CHAPTER 1	8
Introduction to the study	8
Background	8
Research Question	11
Purpose of the Study	11
Chapter 2	12
Literature Review	12
Historical Considerations	12
Relation to other Studies	14
Chapter 3	15
Research Methodology	15
Research Approaches	15
Chapter 4	22
Results	22
Chapter 5.....	26
Discussion	26
Understanding Network Cyber-attacks	26
Chapter 6.....	34
Network Security Implementation	34
Chapter 7.....	39
Security	39
Web Security.....	39
Chapter 8.....	46
Ethical Hacking	46
Understanding Pen Testing	48
Recommendations	57
References	61
Appendices.....	63

DEDICATION

This research paper is dedicated to my daughter *Lindiwe Rapelang Armando* and my Son *Orebotse David Armando* who are very keen in learning information technology.

ACKNOWLEDGEMENT

Throughout my busy schedule including the writing of this thesis, I have received a great understanding and support from the people around me. I would like to extend my great thank you to my supervisor Dr. Rajiv Kumar, who found it fit to guide and assist when I needed his help.

I would also like to acknowledge my employer (committee members of Botswana Union Conference) who allowed me to study while I work. I really do appreciate the trust that they have bestowed upon me, trusting that I will work and deliver my work duties properly while studying.

My gratitude goes to my supervisor at work, Mr. Gift Mpofu, for believing in me and understanding the pressure that I am working under and also extending his helping hand in the work environment, your help is highly appreciated.

Lastly I would like to acknowledge my family for understanding when I was unable to do family duties when I was doing my research. Family times are important, thank you for allowing me to use such times.

TABLES

Table 2.1 Types of Cyber-attacks / Cybercrime.....	13
Table 4.1 Survey Analysis report	22
Table 4.2 – a table showing where policies were developed	24

FIGURES

Figure 1.1 Opportunities of Systems Attack for the Period 1980 – 2003.....	9
Figure 1. 2i Systems Attacks for the Period 2005 – 2014 (Liner Graph)	10
Figure 1. 2ii Systems Attacks for the Period 2005 – 2014 (Bar Graph)	10
Figure 5.1 Example of Network Cyber Attack Using Script Injection.....	26
Figure 5.2 Infection Levels of Rootkit Types.....	31
Figure 6.1: Symmetric Key Encryption Process.....	37
Figure 8.1 Connection Settings.....	51
Figure 8.2 welcome screen.....	51
Figure 8.3 Burp Traffic Recordings.....	52
Figure 8.4 Burp Proxy logs.....	52
Fig 8.5 Burp Interception Request.....	53
Fig 8.6 Burp Interception Results.....	54
Fig 8.7 Burp Interception website.....	54

ABSTRACT

Over the past thirty years, “Network Cyber Attacks” has been an increasing problem in the cyber world affecting organizations and individuals – everyone in one way or the other has been exploited. Ethical hacking and network security can be used to prevent network cyber-attacks in organizations irrespective of their size. Research has proven that cyber-attacks comes as a result of network attacks that are done unauthorized without the system administrators or users of the system being aware of, since the intruders and attackers hide their actions or their presence. The main aim of this research study is to determine how network cyber-attacks can be identified and be prevented to avoid unauthorized access in to the system, access into the private information or data and the stealing of information hence using it illegally, just to name a few. Adding on the existing cyber security attempts, it may ask; Are there any measures that can be put in place to curb the problems coming as a result of network attacks? In this context, Network Cyber-attacks is defined as the accessing of the network services, protocols and network devices unauthorized by individuals or a group of people with an intention to a computer system or any electronic communicative device that has data or information, to harm or to protect it.

Based on the literature review done on network-attacks awareness, a survey was done and distributed to information technology professionals and illiterate personals when it comes to technology. Respondents were given the same questionnaires irrespective of the level of their understanding in IT. The analysis shows a large number of non-IT technical people who are unaware of network cyber-attacks as compared to technical people. The results indicate that network cyber-attacks are a huge problem to people since most of them are not aware of it and how to prevent it if they get attacked or compromised. On this background, it is recommended that individuals and organizations be educated and be made aware of ethical hacking and network security measures and how to use them to implement secure network connections. They can be used to implement secure communications within the organization and communications made outside the organization through the internet or when the system is just idle, they can also be used to identify the systems vulnerabilities.

Keywords; network cyber-attacks, vulnerabilities, ethical hacking, cyber-attacks, unauthorized, intruders, attackers, cyber security.

CHAPTER 1

INTRODUCTION

Background

Andrew Whitaker in his book *Penetration Testing and Network Defense: Penetration Testing-1* has revealed that Hackers were discovered in the year 1969 in the Massachusetts Institute of Technology (MIT), these hackers were said to have been hacking the electricity from trains which were using electricity by then to increase their trains speed. In the 1980 when the computers became popular, people were not aware that computers can be used as tools to commit crime, and when the term hackers immersed and becomes common in the early 90s, they thought it refers to people who are gurus in computer engineering who can be trusted.

There are different threats and attacks in the cyberspace that users or individuals are not aware of which penetrate the system through the networks. Innocent users are prone to be victims of network cyber-attacks, which its main intentions are to get access to the information stored in the systems unauthenticated and unauthorized. A large number of users who fall prey to *cyber criminals* are those who are not empowered to notice and deal with attacks and threats. There are a number of cyber threats and attacks which are very difficult to detect at an early stage of such attacks due to the motives behind the attacks. Those attacks which may be processed without anyone's knowledge are referred to as *cyber threats* or *Cyber-attacks* but for those which can be processed with knowledge are referred to as *cybercrimes*. Restrictions made towards cybercrimes depend on the analysis made properly and on the understanding and behavior of the threats and attacks made to the systems and the users.

There are different threats and attacks in the cyberspace that users of computer systems are not aware of that can be done to computer systems and to the computer networks just to name a few. Cybercrime, cyber terror and cyber war are examples of ways that can be sent to as attacks. To insure the security of such systems is to make sure the computer networks are secure and that ethical hacking is done to ensure the safety of such computer systems. Threats and attacks can be posed by systems that are Outdated systems or systems that needs software updating and systems that are no longer being supported by developers.

A ransomware called *WannaCry* has been seen as one of the dangerous attacks in the cyber world.

Opportunities of Systems Attack for the Period 1980 - 2003

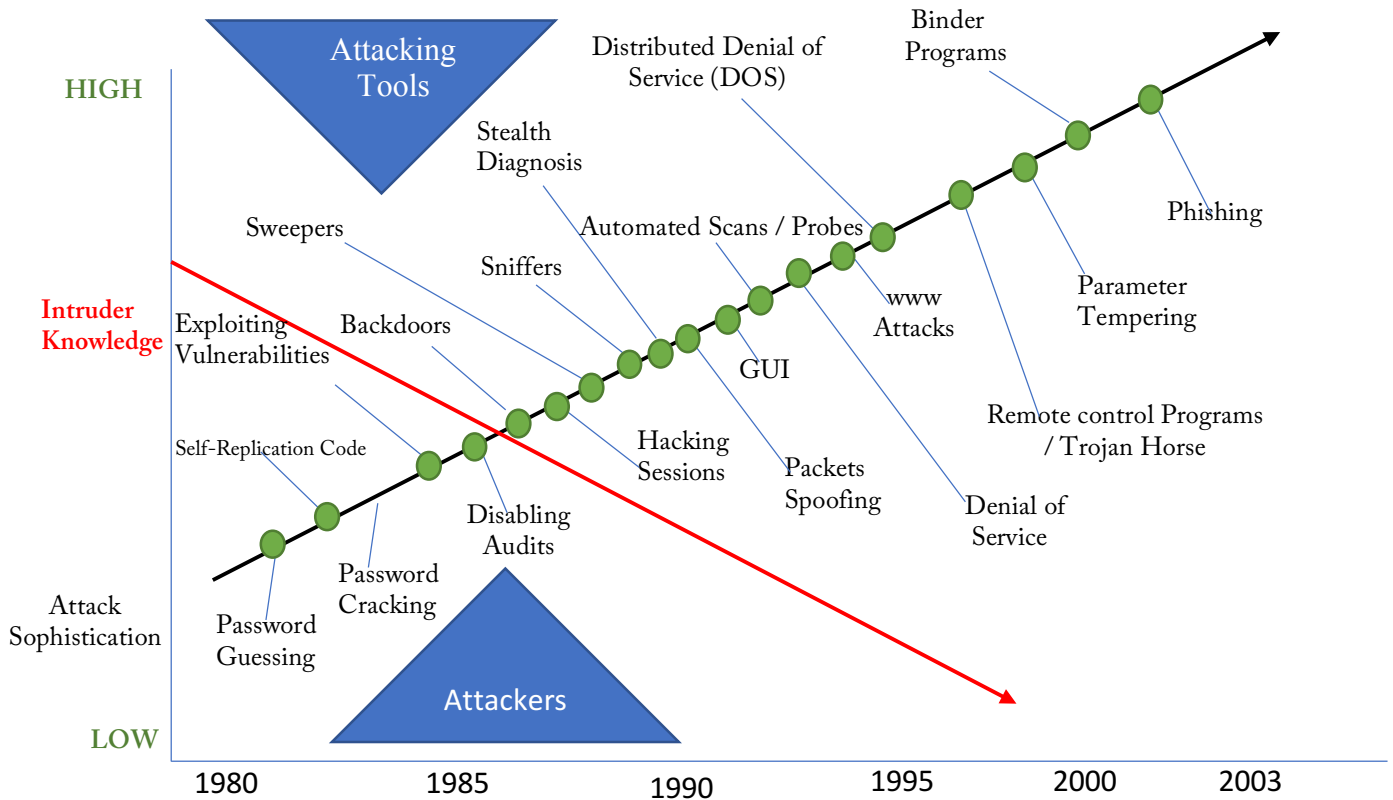


Figure 1.1

The above diagram shows what the intruder use and know to attack the systems and which types of attackers do they systems encounter. Since 1980, the attacks are increasing over the years.

Systems Attacks for the Period 2005 - 2014

The following chart represent the attacks made from the year 2005 to the year 2014 in the united states of America, where we see a major increase over the years in cyber-

attacks with a decline of attacks in the year 2009 but with a high number of files being tempered with or stolen or modified.

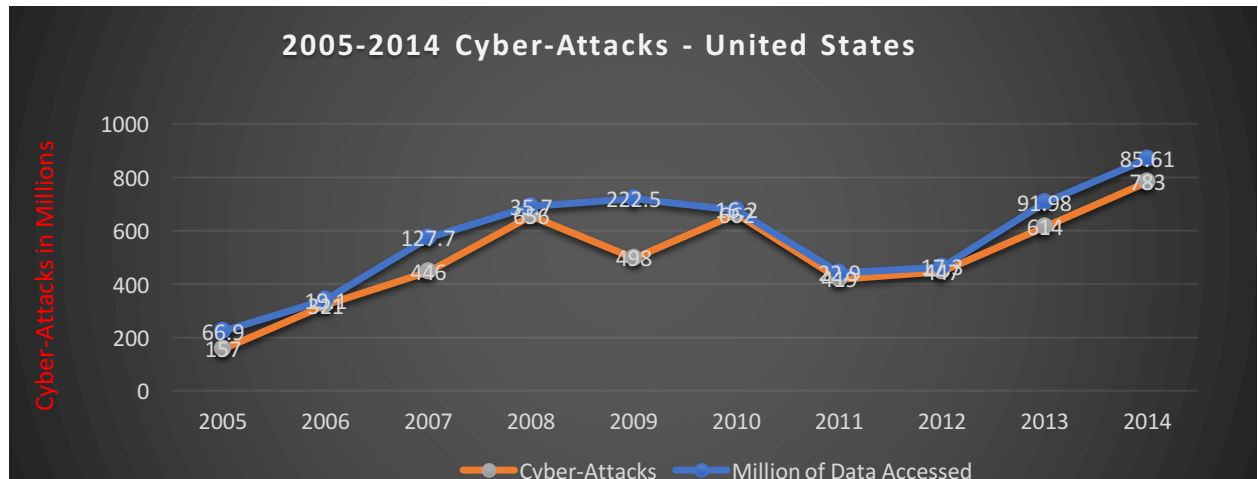


Figure 1.2i Systems Attacks for the Period 2005 – 2014 (Liner Graph)

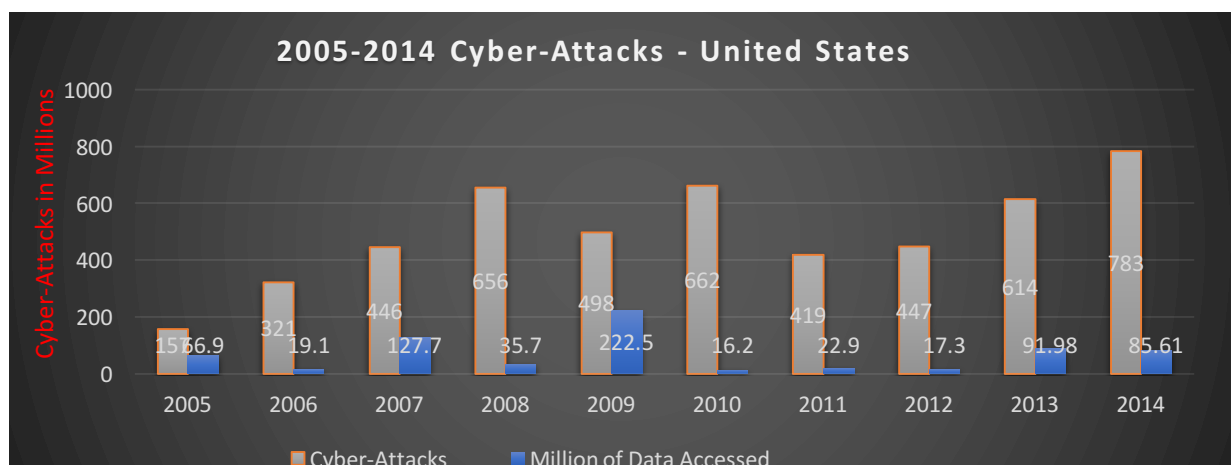


Figure 1.2ii Systems Attacks for the Period 2005 – 2014 (Bar graph)

The exploitation of computers which are vulnerable are highly increasing, in a quicker way hence very risky for all system, taking note that one malicious program or can destroy the whole system.

In today's era, there are millions of people who have access to the internet and we do not have their actual numbers and in organizations employees use computers to communicate using the internet provided, hence this pose a danger to the organization

since anyone can attempt to access the connection to see if its secure. The United Talent Agency (UTA) experience at least one person attempting to get access to their systems in an hourly basis. We turn to say vulnerable computers are large organizations which have their computer systems being accessed remotely since some of these computers have defects in their software's, errors in operating systems, the way they are configured. For an attacker to attack the system, they might have had access to the systems information, that is their IP addresses for instance and most of the tools used in attacking the systems are readily available in the internet.

The need for a better and working solution to this problem is because in the past decades, developers have been trying by all means to stop this kind of attacks but with no success. Different malware detectors like antiviruses have been used to try to solve this problem but with no avail since this problem cannot be solved by using malware detectors because of the way they have been developed and the way they attack.

Research Question

What are the other measures that can be used to prevent network cyber-attacks in organizations and in individual networks?

The main argument is based on the increase of attacks that attack the organizations coming through the network infrastructure of organizations. A lot of funds has been pumped into solutions that seem not to work since there is an increase in digitalized devices and improved internet services. Last year the world was hit by a ransom attack that could have been avoided if the organizations have put necessary measures. This research will discuss few ideas that can be looked into to secure the organizations information and funds.

Purpose of the Study

This research paper comes as a solution to network cyber-attacks by using ethical hacking which has more tools to find and prevent malicious attacks into computer systems at home and in organizations as long as they are connected to the network and the internet.

CHAPTER 2

LITERATURE REVIEW

This chapter will briefly discuss a list of topics which will be discussed and covered in this research project where we will have an overview of the network cyber-attacks and the ways to prevent it. We will look at relevant definition for network Cyber-attacks and relevant terminologies used throughout like Ethical hacking and penetration testing and other aspects of information technology that contribute to network attacks. This will make sure that all the concepts which are relevant to the question for the research are covered and that all the gaps are identified and explored within the existing research environment, so that the research question is well understood.

HISTORICAL CONSIDERATIONS

Cybercrime can be defined as “any crime that is facilitated or committed using a computer, network or hardware device” according to (Gordon & Ford, 2006). This term is used around the world but people are failing to get one definition for it but the definition evolve around the same words with the same meaning. Over the past few years’ researchers have been failing to classify this term but writers like (Ngafeeson 2010) proposed a model which is motivational which can be used for clarification purposes with the intention to stop cyber-attacks. (Poonia 2014) concentrated on the challenges that comes with network cyber-attacks and came up with a proposal of classifying this problem into 4 categories being; the victims of the attacks (like crimes which target individuals, crimes which concentrate on the organizations and its property or the government). The other studies that can also be looked at are the (O’Neill, Aiken, Haughton & McMahon, 2015) who specifically concentrate on cyber-attacks and (Stol & Veenstra, 2015). (Ford & Gordon, Jaishsnkar & Ngo, 2017), once had a discussion that was deemed to not exist by other researchers. But that did stop them from continue with the research, they said there are other terms which are used interchangeably unknowingly with cybercrime, which are *internet crime*, *cyber-attacks*, *electronic crimes*, *computer crimes* and *online crimes* just to name a few. The following is a figure that illustrates the different types of crimes or cyber-attacks;

TYPES OF CYBER ATTACKS / CYBER CRIME

HACKING	Email hacking Password Hacking Computer Hacking Network Hacking			
EMAIL CRIME	Email Spamming Defamatory Email Email Threatening	Email Fraud Email Bombing Spreading Malicious Code through Email	Email Forgery Email Spoofing	
CYBER TERRORISM	Cyber Extortion	Cyber Hate Cyber Harassment	Cyber Vandalism	
CYBER SQUATTING	Copyright Infringement Software Piracy		Trade Mark Violation	
FINANCIAL CRIME	Credit Card Fraud Salami Attacks	Cyber Laundering Selling Illegally Gambling Online		
IDENTITY THEFT	Vishing	Phishing	Pharming	Smishing
MALICIOUS CODE	Virus	Multipartite Macro	Boot Stealth	
	Worm	IRC Network	P2P Email	Internet
	Password Attack	Hybrid Dictionary Keyboard logger Brute force Network Snooping		
	Trojan	Proxy/Wingate Trojan Key Loggers Trojan Destructive Trojans Password Sending Trojan Remote Access Trojan		
	DENIAL OF SERVICE			
DATA DIDLING				
CYBER STALKING				
CYBER PORNOGRAPHY				

Table 2.1

With the above table demonstrating different types of attacks, it becomes easier to understand the different ways networks are attacked and it becomes an easier way for the debate to affirm that a better way of preventing cyber-attacks is needed.

RELATION TO OTHER STUDIES

Attackers

One may need to understand what is meant by an attacker or a hacker, these are individuals or a group of people who access the systems when they wish or want without proper authorization but according to (Jargon file 4.4.7, 2003), which has different versions of defining an attacker, it sees them as those people who tempers with the security of the system while the community sees hackers or attackers as good people. More understanding of these can be seen in separating white, black and grey hackers from each other, not forgetting to look at the hacktivists who got discovered in the early 2000 with a lot of misunderstanding and anonymity. (Hampson, 2012) says there is “*the nonviolent use for political ends of “illegal or legally ambiguous digital tools” like website defacements, information theft, website parodies, Dos attacks, virtual sit-ins, and virtual sabotage.*”

CHAPTER 3

RESEARCH METHODOLOGY

This research chapter or section will give a discussion of the methodologies used and the paradigms and those found in the Information Technology used in this research. The discussion will also include those methodologies which were employed throughout the process of this research documentation, together with the discussion and presentation of the procedures used. The initial literature that was collected is also included in this chapter.

Research Approaches

According to research, there are several numbers of different paradigms used in the underlined research done in information technology (Clarke 2005). According to (Kuhn 1970) paradigm is *“the underlying assumptions and the intellectual structure upon which research and development in field of enquiry is based”*. Patton defines paradigm as *“a world view, a general perspective, a way of breaking down the complexities of the world”*, (Patton 1990). It will include the positive side and the interpretation, the quantity and the quality, those which are deductive and inductive, and those which confirms and make explorations. A paradigm can be used to serve different number of purposes which can be understood to;

- Guide the technical people or professionals to indicate issues that are important used to challenge different disciplines.
- It can again be used to develop theories and models that will enable testers to solve problems
- It gives procedures, methods and principles to be looked into when similar problems arise
- It sets criteria for instruments, data collection methods and methodology used for solving such problems.

The difference between Quantitative and Qualitative Methods

These are the main research methodologies that are used to conduct researches. Qualitative research is a research method which is used to confirm the theories and explanations hence it is a standardized method of data statistical analysis and data collection. It uses structured interviews and closed ended questionnaires to

collect data, and its findings are based on the numbers and responses which are definite from the research participants. Its main research findings are based on the initial plans of the research which makes it to be easier to analyze and interpret its findings. Qualitative on its own revolves its main focus around how qualitative data is being used – interviews, observations and published documentations. Its main objective is to answer questions which its findings do not come as a solution in the beginning and it usually give results or findings that are used beyond the research process. It is identified by having exploration, discovery and induction characteristics where the researcher is the main thing in the process in building the theory and collecting of data. It collects its data or information by doing deep rooted interviews, having focus groups and research that is grounded.

These 2 research methods are paradigms which its main base is on positivism interpretism juxtapositions. This paradigm – quantitative; its research is based upon positivism which has a position which its mandate is to advocate for the independent existence of how human being think. There is a separation between the researcher and the object in question so that they do not give influence to one another. It also gives research which is empirical with the believe that all findings can be subjected to empirical factors which will be representing the correct information or the truth. Usually the techniques used to the research includes rules which are structured, surveys with expected responses and information randomization. Qualitative research results are usually smaller than of Quantitative research findings. However, the qualitative paradigm is wholly based on the interpretivism, which will allow it to collect human beings mind outcomes. The research made and the researcher are seen to be independent from each other hence the findings on its own are mutual to its content.

On the other hand, a mixed approach (a combination of qualitative and quantitative approach) can be seen to be of waste of time since it requires a lot of time hence it has a likely hood of producing more informed data or information. It normally occurs when there is a collaboration between the researchers who allows the use of different approaches, concepts and techniques from qualitative and quantitative methods. It includes the induction, deductive reasoning and the inquiry methods, this will allow researchers to understand the

weaknesses and the strengths of these approaches and how to improve it to have a better study design as the outcome.

There has been an argument on combining these research approaches which has come to a solution to many problems. Researchers like (Sale et al 2002) have a great argument that these two paradigms cannot be combined looking at the fact that they do not study the same things or ideas, therefore they cannot be used in purposes such as triangulation and cross validation; but other researchers saw a different point and they were arguing for their combination since these methods do not have the same strengths hence combining them will give more reach results as compared to them being isolated. In the other hand (Morgan 1998), thinks that combining them could be done in aspects that are technical.

There have been different ideas how these methods can complement or be used together. A suggestion has been made by (Johnson et al 2007) that, the design stage of the research qualitative and quantitative can complement each other by identifying objects that were not identified and also identifying samples that are left out. (Creswell 2003) has a prerequisite of having research design being combined throughout the design and processes implementation whereas (Maxwell & Loomis 2003) have a different view to this approach which is having approaches to the mixed being different from other approaches by having a research design which has components being separate from each other, being its purpose, validity strategies, conceptual framework. Research questions and methods used.

The following is a discussion showing other methods of information or data collection which are found in the qualitative and quantitative research which I also used some in my research, which will discuss its weaknesses and its strengths.

In-depth Interviews: this is where there is a direct communication between the interviewee and the interviewer, with an intention to get information that is more detailed which can be of importance to the research.

Advantages:

- Normally rich content of information is collected with current and insights that are valuable.
- Allows the benefit of face to face interaction.
- The researcher gets the experience of the collecting cognitive responses and experiencing its effects.
- Questions are explained and clarified for easy understanding by the researcher.

Disadvantages

- Time consuming and expensive
- Qualified and well trained researchers (interviewers) needed.
- Desire to impress the interviewer may make the interviewee to distort information being collected.
- There can be flexibility which can make the interviewer to be inconsistent.
- More information can be gathered hence it can be very difficult to reduce.

Observation: these are methods where researchers have access to information first hand either on studies being conducted (behavioral studies), processes or either on programs.

Advantages:

- Direct data is being provided either on individuals, programs or in groups.
- It exists in environment which are unstructured, flexible or natural
- Good opportunity for outcomes that were unanticipated.
- The researcher is able to easily understand the environment or the situation or the context of the research.

Disadvantages

- It requires a lot of time hence it is expensive
- Needs highly trained or qualified or content experts during observation
- The behavior of the participants may be affected by this process
- The researcher or the observer or the investigator has limited or no control
- The perception of the selected observers may have the information or data being distorted.

Focus Groups: A combination of observation and interviews in one setting

Advantages:

- Easy and quick to set
- Used mostly in groups and it allows easy observation of such groups, their discussions, behavior and maybe their language.

Disadvantages:

- Researchers might be biased to a certain group
- Few individuals might control the discussions of the group while others don't contribute.
- Analyzing data from such can take a lot of time hence they should be planned well ahead in time.
- Valid information may not be provided.
- Data may not reach other groups in a correct format.

Document studies: Records which are existing may be used to provide information to groups of people where there is no provision for observing.

Advantages:

- Very cheap and information is readily available.
- Customized to the environment where research is done.
- There is an opportunity to study the research objects trends over time.

Disadvantages:

- The research may be not completed.
- Its authenticity can be questionable since it is not accurate.
- May not be easy to locate documents needed.
- Might take time to analyze the findings.
- Access to such information is not easy.

Difference Between Interpretism and Positivism

In the research approaches, there are just a few metaphorical differences between them (positivism and interpretism). (Stahl 2008), states that in ontology which deals with the study of being and becoming; interpretism assumes that reality and the researcher cannot be separated while positivism assumes they are separate. Epistemology is the study that deals with the theory of knowledge or just knowledge, Interpretism assumes knowledge

is gained through the experience of living or just interacting with the society while positivism believes there is an existence of objective reality which is more than the human mind. In relation to what has been researched, interpretivism believes the object being researched on, its interpretation is linked to the researcher's experience with life as compared to positivism which believes the object in question has its own qualities that are not connected to the researcher in any way. In trying to get information or data concerning the object being studied, interpretivists will use phenomenographic, hermeneutics, ethno-methodological studies, case studies and ethnographic studies as the methods used in the research to understand the results they got which are indirect and also consider results that have hidden meaning while positivism uses different ways to gather information which can include field experiments, survey and lab experiments hence this will enable it to gather a large number of information needed which can be needed to engage statistical analysis which can be used to detect any irregularities in the study. In research, the validity of the measurement of the research should by all means refer to the broader way in which the research wants to measure, what it also wants to receive as opposing to the views that can be obtained from the interpretivist and the positivist. The data collected by the positivists at all times are said to be the true measure of the research reality hence they tend to get information which is valid. In the positivist, the approach engages different ways of checking the validity such as statistical and construct validity conclusion together with the external validity and the internal validity. On the other hand, the interpretivist are the ones who are concerned more than the others concerning the knowledge which is being collected from the research being conducted hence wants evidence to be available for everyone to support the claims made by the researchers. And again, they will want the contents of the findings of the research and the research process being used should be used in making the decision to accept the findings. The positivist on their side believe that the findings of the research are reliable if its outcomes are found to be the same only if they are done by other positivists. Reliability is lacking in them - According to (Joppe 2000), *"The extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability to factors such as researcher bias, errors in measurement, and inconsistency of the procedures used"*. However, the Interpretivist have made a suggestion that a research can only be reliable only if the researcher can be able to demonstrate or make awareness in interpretive.

(Weber 2000) wants to believe that these differences in meta-theoretical are said to be false when looking at the differences between the approaches, he continues to believe that the difference found only depends on the method being chosen. Positivism researchers only use the field study, surveys and the experiments methods to get their research findings while interpretivist researchers are inclined to using the studies such as case study and the ethno methodology. The difference between the positivism and interpretivism research methods choice can come as a result of factors influencing such as the type of training being provided to the researcher, or the recommendations made from the advisors. If the methods can differ in any way, the main aim of conducting a research is to get findings that can be used.

CHAPTER 4

RESULTS

At the end of the survey period the researcher received 75 responses out of 90 who were distributed with 69 responses being useful. Out of these 75 responses 2 respondents just answered the first question and the third question which wanted to determine if the person was connecting to the internet or not and if they have devices to use to connect to the internet. The other for 4 questionnaires were not completed, not all questions were answered.

The main aim of the research was to find if people who connect to the internet and the networks at work areas able to identify threats and attacks when they come to them. The results show that just a few understand and know what network attacks are and a large number of people are clueless. These are just information technology people and those who work in the computer environment who include secretaries, officers, Human resource people and others. The following shows a table indicating the background of different respondents in the research;

Background in different Organizations with no cyber-attacks knowledge	Level of Network Cyber Attacks understanding %	Educational background in IT
IT Personnel 5%	8	12
Secretary 35%	0	0
Human Resource 30%	0	0
Officers 20%	0	2
Others 10%	1	8

Table 4.1- Survey Analysis report

As indicated in table 4.1 above, we found out that 5% of information technology people are aware of network cyber-attacks while 35% which is of secretaries do not know a thing about these attacks, which is a risk because almost all the communications of the organizations are dealt with by them. 30% percent was for human resource personnel and 20% for officers while 10% constitutes to the other staff of the organization. 95% of the people constitutes to not understanding anything concerning network cyber-attacks which is very important to our field of study. This demonstrate that most of the organizations are not secure since the computer systems are not taken care of people who are not qualified enough to protect the organizations systems. Even though it is the consensus in most organizations that anyone who can switch the computer on and off

can be seen to be the person to take care of the systems even though they are not well trained for that, poses a lot of our organizations in danger of well-trained hackers who know what they do and want. The results of the survey show that a majority of the people who are indulged in these systems are well empowered in this area and it comes as no surprise to us if we see the statistics of cyber-crimes being committed each and every day and where we see a lot of policies being implemented by governments. It also indicates no efforts in organizations who wants to train their people in this object of study in order for the control of network attacks.

The researcher wanted to check the experience of the people in the field and their experience, their background experience when they have been working in this field as people who wants to take care of the security of the organization. The survey wanted the respondents to state their experience in the work as long as they have been practicing, those who were under five years in service were the Information technology, followed by others who spent less than 8 years in the work, secretaries and human resource personnel's with ten (10) to fifteen years in service and lastly the officers with a arrange of 20 to 35 years in service, you would see that the people who are supposed to be taking care of the system are not that experienced as compared to the officers whose main job is to take care of the organization in the managerial side. The organization can only depend on the 5% which is not well experienced in terms of security.

Network cyber-attacks has been a problem over almost every country and every organization as long as its computers are connected to each other over the internet and the network. To determine if the people are ascertaining with the concept of cyber-attacks, question 26 asked the respondents to give a definition of cyber-attacks according to their own understanding. A few attempted to answer this question though the majority decided to leave the question as it is, which shows a lot of them do not know or understand this term. It must be noted that the majority of the people do not know what these attacks are.

The statistics and the literature review published shows that there have been a major increase network cyber-attacks over the years. And there have been different attempts in trying to curb these attacks over the past few years which left so many organizations with a lot of money being lost due to cyber-crimes and a lot of money being invested in antiviruses. To rectify or quantify this observation or this assumption, questionnaires

were used to find out from people (specialists / information technology experts) involved, the way in which their services are required, how frequent (question 10). The response we get was that there is a need for cyber security implementations since they responded by stating that their services are needed time and again, that it is hard to state the frequency since they never stay idle without scanning a computer for possible threats or attacks.

Another objective to this research was to find the state of the systems attacks which are current, its procedures, its existence and if there will be a need to implement it and to check if there are standards set aside for that. Are there any other policies set aside for each organization and if there are other tools that are used to fight this problem.

	YES	NO
Does the organization has any set policies which can be used in guiding the security of the networks	13%	87%
Where these policies developed	0 0 35 13 52	
In house		
From other developing organizations		
Adopted from other organizations		
From organizations that develop antiviruses		

Table 4.2 – a table showing where policies were developed.

Table 4.2 above was used to find out if there were any policies set in place to guide where there are attacks in the system which showed that 87 % of organizations do not have policies set in place for curbing the attacks in the organizations while 13% said they do have policies set in place for their organizations.

Summary

This research was based on grounded theory that is qualitative research and again included the quantitative or questionnaire methods with 3 stages being used during its process, being the initial survey in the literature which was used to identify the omissions and the gaps in the ideal plan for controlling the attacks initial plan. Data was gathered

from the people in the field as the next step then the last step was to distribute the main idea for testing and implementation. The results of what seem to be a solution to this problem is being discussed in the following chapters.

CHAPTER 5

DISCUSSIONS

Understanding Network Cyber Attacks

This research build on the exiting knowledge that a cyber-attack in computer systems and computer networks is said to be any attempt in exposing, editing, deleting, stealing, destroying, disabling, using or gaining access to confidential, sensitive, private and protected information or devices unauthorized. Network cyber-attacks are any inappropriate behavior which makes its main target in computer networks, network infrastructures or any communicative device connected to the internet to manipulate its stored data. People or applications which has an intension to access any restricted information or any device without authorization with the intension to manipulate the system through the use of malicious software are referred as Attackers.

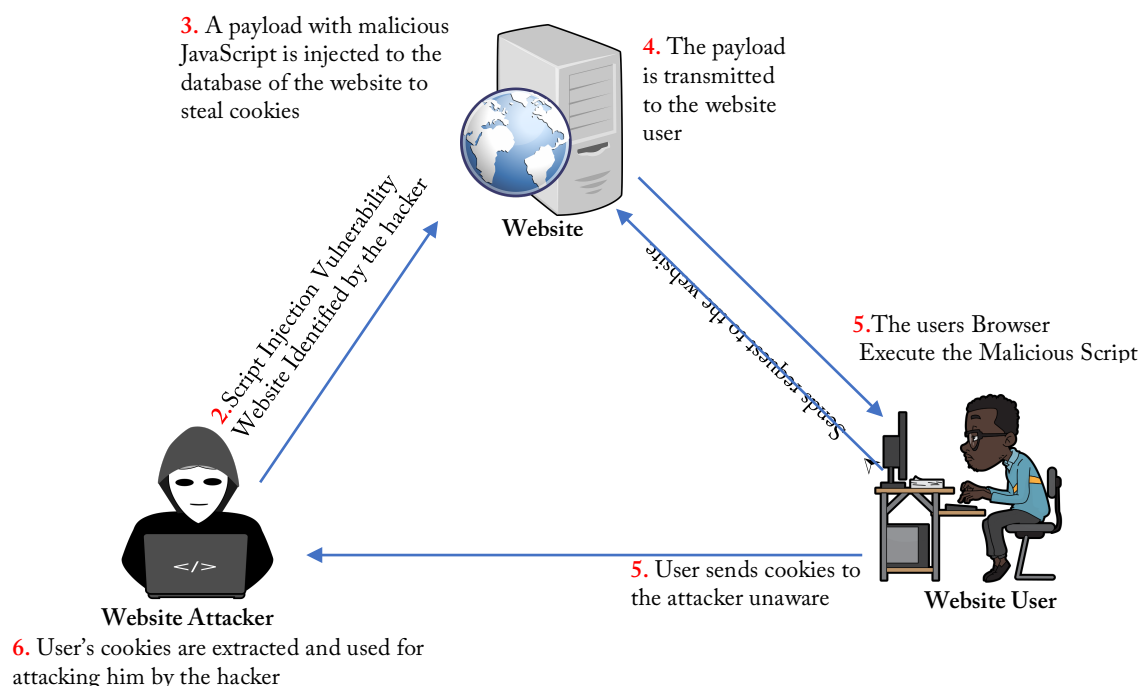


Figure 5.1
Example of Network Cyber Attack Using Script Injection

A cyber-attack can be from any source either from individuals, organizations or from the governments and can be categorized into cyberwarfare and cyberterrorism.

5.1 CYBER-ATTACKS CATEGORIES

Cyberwarfare: It is where a computer systems technology is used to deliberately attack / disturb or disrupt activities from a certain organization or the state of the nation by attacking its systems which stores information used for strategic matters or information or data systems concerning the military. One of the tools used to prevent such attacks is through the use of *Penetration Testing*, which can be used to prevent attacks formed against network infrastructure, to minimize the recovery time and the damage made from cyber-attack and to reduce the vulnerability done to cyber-attacks.

Cyberwarfare can be of the following types, ***Espionage***: which is a practice used by states to spy on military or confidential or secret political information or data without the authorization from the owner of the information. They can be Government attacks or Corporate attacks, ***Propaganda***: Which is a psychological warfare which uses digital devices to control data in any way to make influence to the people concerned and ***Sabotage***: this is an attack or a malicious act that can be contracted in the internet or through deliberate physical installation to the desired machine or system. *Cyberterrorism* is a politically based motivation in the use of information technology intelligence and the computer systems to make an intentional fear or disturbance to the society.

5.2 TYPES OF NETWORK CYBER ATTACKS AND COMMON SIGNS

Defacements; This is an attack where attackers replace the contents of the website attacking with their own contents, that is their logo, their names or even their contacts.

Ransomware:

“Ooops, your files have been encrypted”, “Payment will be raised on”, “Your files will be lost on” are a bad sign that you have been attacked by a Ransomware known as “WannaCry”. These are malicious software’s that gain access to the system by locking access to the files of the system with a certain amount of money needed to rescue the whole system or some certain files. The target is mainly for large organizations that have a large number of files. Bitcoin is used as a currency to rescue the files or systems held at ransom, untraceable ways of paying attackers is used so that they cannot to be traced.

Distributed Denial of Service Attacks (DDoS attacks): Automated and illegitimate traffic is used to flood the website in order to make the loading time of the system slow with the intension to crash or take the entire website down or offline. In a day, an average

website can take 8 of DDoS attacks because it is cheaper and easy to execute. They are identified by slow systems, slow to load websites or where websites crash instead of opening the desired website. **Backdoors:** A malicious entry point for network cyber attackers, which are left open so that they can come back and enter again unnoticed. 23% of website infected files comes from backdoor attacks hence so difficult to detect them but if the signs of a backdoor attacked website are known, it is easy to identify, with images disappearing from the website and high bandwidth usage reporting. **SQL Injection (SQLi):** It is an injection of SQL statements which are malicious into input fields of the current user, like account sign in form. Customers data is stolen, edited, modified or even deleted once the attacker has gained control of the website. An entry point of such an attack can be where forms are not protected with tools like entry codes or image identification security. Disconnected Content management systems, changed passwords for databases, new administration users being added can be a strong sign that the website has been attacked with SQL injection.

Cross-Site Scripting (XSS): Malicious pop-ups and websites redirects are a great sign of this network cyber-attack. Codes which are malicious are injected into client's websites as a form of a network attack, these attacks look at the security flaws of the website and make a move into attacking such a website. **Malvertising:** This is another form of attacking which uses deceiving and malicious advertising to spread malwares. Like the above attacks, this attack also injects malicious codes into the advertisement that is legitimate or by using the real advertisement as a way of delivering attacks or threats. The spreading of this kind of attacks is done when the user accesses the advert and the malware automatically download and installs itself in the user's computer or system.

Phishing: These are scams used to deceive email users to disclose their personal details such as an invitation to participate in a completion, obviously, the email user will be asked to provide information like username, passwords and bank details. In this case the attacker has every information that they need to access your system. There are several things to look out for when dealing with emails, which can easily state if Phishing is going on; It always uses an email, it may provide a link and ask for validation or update of information by accessing the provided link, its awards are always promised and in most cases, it directs you to a fake website which looks real and legitimate.

Bad grammar may be found there, it may also include malicious attachments which might have a link or a file extension and at the same time it might look like it is from a well-known company/ Your Bank / any Government department which will ask for your name, your employer, your address, your phone number, bank details or date of birth. There is another type of Phishing which is known as spear Phishing which convinces the email user that the mail received is the legitimate mail since it may have signage as similar to the one your boss uses at work, or from someone who has been saved in the contact list, email from work / from a friend / from a business deal the user is in. The main aim of this attack is to make sure the owner of the email provides more of their personal information which will allow attackers to have full access and ownership of your email account. There are several ways that the user can protect themselves when suspecting they are being attacked; They should not open suspicious emails, or they should not access provided attachments or links which look suspicious to them. They should not by any means provide their personal details or any information when they are suspicious. Telephone numbers are at times provided, they should not call those numbers, Check if digital signatures are there in the mail, Suspicious emails should be deleted immediately, the security Systems administrators should be contacted should there be any suspicion and malicious domains and Malicious IP addresses should be blocked as soon as possible. Intrusion Detection Systems (IDS) should be configured and be used and any suspicious incidence should be reported.

Redirects: this is a redirection of a link to a malicious link when the website user tries to access a legitimate website, this will leave the website and the computer system being infected by malwares. To know if the website has been redirected, the desired Uniform Resource Allocator (URL) will be redirected to a suspicious different URL or site. ***Search Engine Optimization (SEO) Spam:*** These are a set of various techniques which are used by network administrators to have websites have desired better results when querying them. It uses keywords placed in the web copy and backlinks from other sources which authorize the concerned website to access required words. The more the links point to a certain website, the more the outcome from it and the more vulnerable it becomes. The spam will take advantage of such links and send malicious backlinks also to a site sending a request. Traffic can be stolen and be redirected to a malicious website which is similar to the one requested. Signs of an

attacked website by this kind of a spam will be; unusual appearance of links in the open site, loss in traffic and suspicious links and comments posted in the owner's website.

Malware: The attack is made with an invitation to download the latest software that will be used to remove the spyware since the system is infected. Its main aim is to destroy the computer systems. Types of Malwares include Virus, Exploit Kit, Adware, Spyware, Worms, Remote Access. **Rootkit:** They attack the computer systems through structured layers of the computer so that they can hide and become undetectable. Modification in this attack can be done only in the same level the malicious is found. The BIOS is the most vulnerable to attack since most of the time the security do not protect it. It can be used to listen to the internet traffic of the user, hide other malicious malwares and at the same time it can enslave computer systems to be into botnet. **The effects of Rootkits in the Operating System:** Rootkit behavior is dependent on its developer's intention; it makes sure it provides its developer or the attacker with a computer systems root access where installation was done. The attacker can now have all the admin rights of the computer once they have access to the whole system through rootkit. Application programming interfaces (API) calls are being intercepted by the rootkit like sending a request to internet windows explore – file manager programs. Kernel rootkits can be created at times to manipulate and modify the correct components of the operating systems kernel and corrupting it at levels that the real rootkit can easily identify the attack.

Rootkit Hypervisor: Similar to the rootkit since they both gives the attacker the privilege and control over the infected computer system. The difference can be that this one is a virtualization software layer which operates between the hardware and the operating system, pretending to be a monitor for a virtual Machine (VM) hence allowing running of multiple OS at the same time in the same processor. But this is a great danger since its operation is dependent on the original OS running in the VM.

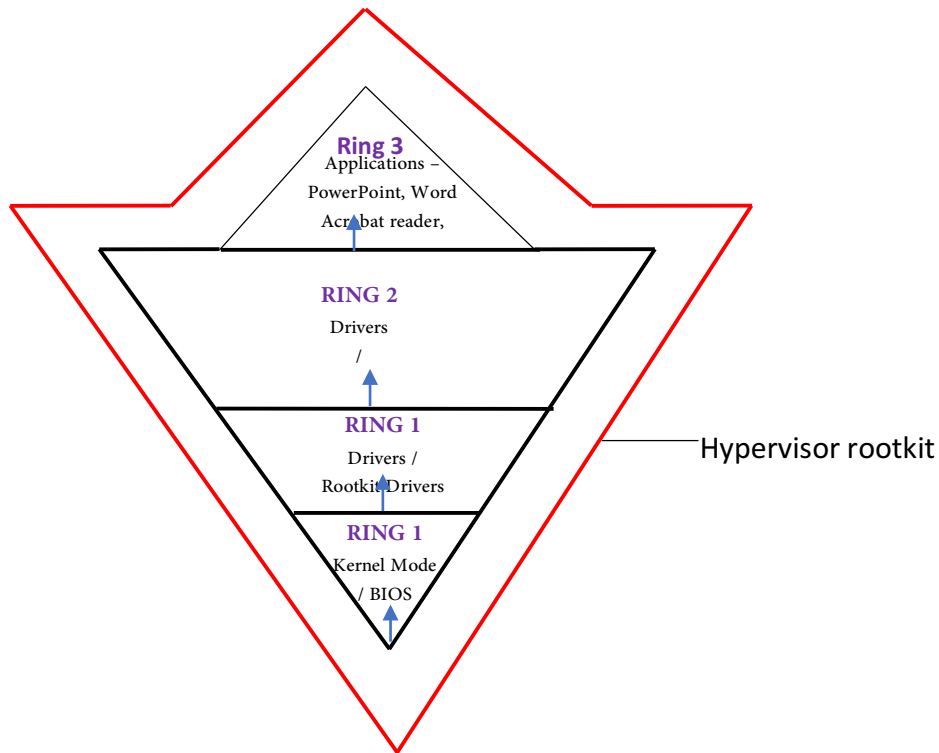


Figure 5.2: Infection Levels of Rootkit Types
Hypervisor rootkit Network Connections

Default Passwords: A password is meant to enforce the security of a system, to authorize and authenticate who can have access to the system, but passwords which are easy to guess, weak and default passwords pose a great danger to the system. A weak password can be seen by using the systems users first name, their date of birth, their marriage date if married, using words which can be found in a dictionary or passwords that do not have special characters in them or that do not have upper caps in them. Same passwords that are used across all websites and systems to login also pose a great danger to the system. Users can be advised on how to create strong safer passwords by considering the following; Never write down the password, Login credentials should never be saved in a browser, Make a habit of changing the password time and again, Make sure the account log you out if the user has more than 3 failed attempts to access the system, Common words or phrases should be avoided when creating a password, Personal details or information should be avoided when creating a password, Diversity of characters must be used, that is upper case and lower case letters and special characters should be combined to make stronger passwords.

Outdated Software's and unpatched Software's: Software's that are outdated which needs to be updated can be vulnerable to cyber-attacks. Unpatched software's and systems that need to be updated can be seen by having so many unauthorized activities such as, unauthorized computer system information disclosure, access attempts, transmission or storage of data or unauthorized modification of software and hardware components attempts or succeed. To avoid these attacks, the systems users must comply with the policies set to safe guard the organization computer systems, always make sure that the systems are up to date with the newly released software patches and software updates. If there is a suspension of an attack, the system should be disconnected from the internet and the network, to avoid it spreading to other systems and that the malicious attack can be easily controlled. Make sure that the system has active firewalls and antiviruses.

Removable Devices: This refers to any storage device that can be removed or attached to computer system to transfer information or data from one computer system to the other. These devices if they are not taken care of they can breach the security of the system hence they need to be scanned of malicious software's before they can be used, these are one of the devices that pose a greater danger to systems since they carry one malicious software from one computer to the other. These are; CDs, DVDs, Flash Drives / USB, Thumb drives, External Hard drives and phones which can be connected as a storage device to transfer and store information.

Hackers and systems attackers may leave these devices at a certain location where they want to hack, maybe in the accounts office, so that people in the accounts office can pick it and use it. At times these devices are given for free as a customer buy certain goods / devices. Once the user attach the removable device to the computer, the system will be infected hence files or data stored can be damaged or destroyed or hackers can have access to the system unauthorized. For one to protect themselves against such malwares, they can make sure they follow their organizational policy regarding removable devices, they are not supposed to use flash drives unless authorized to do so by the system administrator. Any personal removable device that is personally owned must not be used in the organizational system and at the same time the organizational devices should not be used in personal systems. All data stored in such devices should be encrypted to prevent editing of data during transmission.

Malicious Codes: These are malicious software's which have unwanted behavior with its results being damaging or creating what is not expected, such software's includes; Worms, Backdoors, Viruses, Rootkits, Trojan Horses, Key-loggers and Spyware.

The system administrators and the its users should be aware of the following suspicious behavior; its files will corrupt with modified data or information and the data might be lost due to interruption. Tempered systems might be hacked by many hackers hence ending up being sabotaged. These kinds of malwares can be distributed by various kinds of ways, that is; Downloading infected files, accessing websites that are infected, using removable devices like USB / DVDs, receiving email attachments that are infected. To prevent and guard against such attacks, the systems administrator should take a few security measures against such especially in emails and websites. In Websites; The administrator should, block any links and IP Addresses that are seen to be malicious and make sure that all protocols and services that are not used are blocked.

CHAPTER 6

Networking Security Implementation

Network attacks has exploited the vulnerabilities of many computer systems hence they have been a rise since but just a few gets discovered.

6.1 Common Network Vulnerabilities

According to ICS-CERT the worm called *stuxnet worm* has been operating for more than three years since 2010 without it being detected. The main danger that this worm imposed was to destroy the network infrastructure. These attacks can be categorized into protocols used in communications, applications and platforms, procedures and policies, and network attacks where our main concentration will be on the network attacks.

6.2 Network vulnerabilities: this comes mostly due to the network configurations made, the type of hardware used, the monitoring of perimeters, the wireless connections or even the authentication of communications made with the following to look at;

- i. No backups being made or when the network settings are not stored.
- ii. No firewalls or firewalls not being configured properly or when the firewalls are missing.
- iii. Inadequate settings of network controls.
- iv. No network traffic monitoring tools.
- v. No data protection tools like encryption protocol.
- vi. FTP or Telnet protocols used without implementation of encryption mechanisms.
- vii. Integrity not implemented hence there is not constant check on devices.
- viii. Security borders not clearly defined.
- ix. Physical ports which are insecure are being used.
- x. Network passwords are poorly managed – default passwords used, use of passwords being unencrypted, passwords which are never changed time and again.
- xi. Poorly managed authentication mechanism found between access point and the wireless client.

- xii. No security measures set in place for the network architecture designed.

6.3 Network Protocols: most of the network attacks comes as a result from network protocols vulnerabilities used in the communication either wireless or wired. Attacks like Man in the Middle, Denial of Service, lacking of authentication to messages and encryption are protocol based.

A buffer Attack: it is a continuous memory which is allocated for a certain process which will be used to store its data (process or application). The process called buffer overflow only occurs when data which is written is used to corrupt the address values which are adjacent which are allocated to the buffer if there is a problem of insufficient space. Program hijacking by the attacker is due to control data path being overwritten hence allowing the attackers to make their own move to attack.

6.4 Network Security Policy

A secure security policy should be kept in place to make sure that the data is kept secret or secure, that is sensitive information should be only made available to those who need to access it. Customers information should be available to the relevant people not to everyone. Information should only be realized when authorized to be by relevant people like officials or lawyers. A secure system will need a policy that will minimize or stop all the attacks or threats of leaking information or data to any unauthorized personnel's or applications. Network Policies makes sure it prevents unauthorized applications from revealing confidential information accidentally or from accidentally learning confidential data like credit card numbers. The main aim of security policies is to keep information that is sensitive confidential.

6.5 Firewalls and Proxies

Firewalls and proxies are used to control access control from any direction the attack may be coming from. The firewall is used to control access to the network by disallowing or allowing certain access to the system depending on the policy set. The policy also can help the firewall to reject or accept messages based on the information provided such as the ports or destination IP addresses

not on what the message contains. A firewall known as filtering firewall allows access control based on different attributes of headers packets like, source address, source IP address and destination IP address, e.g. routers and systems infrastructure. Outer firewalls are used to restrict access from the public to the organizations network computer system to the internet.

A proxy is a server or an agent which does not allow a direct connection between two different points on behalf of the endpoint. Or we can say it is a firewall which performs access control through the use of proxies. Access control can be based on messages and packets and the attributes on different header packets. A filtering firewall gets its ability from a proxy firewall to base its content on the packet levels or levels of abstraction which are higher.

There are three type or methods of penetrating the firewalls by the attackers which is through the use of web server ports, through SMTP ports and lastly through by passing the low-level firewall. When using the webserver ports, the attacker use the unsecured port – HTTP proxy to check for illegal HTTP requests or for requests that are invalid hence it will reject them. The mail server proxy will detect such attempts and rejects such illegal or unauthorized attempts.

6.6 Cryptography

A secure method for preventing interception during communication and protecting data or information malicious activities during its transmission to allow the intended person to read and process it. Encryption is part of cryptography which uses keys and algorithms for transforming plaintext (input text) into a Cipher-text which is an encrypted output. Algorithms are used for transforming the given plaintext into the same encrypted output when the same key is used throughout. Algorithms are secure since they make the attacker not able to get the properties of the encryption key or the plaintext when they have the cipher-text. Algorithms do not allow the attacker to find any information about the encryption key combination when they have cipher-text or plaintext. Cryptography can be sub divided into symmetric and asymmetric cryptography.

6.6.1 Symmetric Cryptography

The same key is used in encryption and decryption hence it is cheaper to design a strong symmetric key to encrypt with and algorithms to process. Symmetric keys are not that big to when produced since the area it secures is not that huge. Its implementation is highly effective due to the fact that the developer does not have to deal with time delays during decryption and encrypting. It also allows authentication since data is encrypted with the same key that is used to decrypt the same message. As long as there is privacy in keeping the key (by the sender and the receiver) which is used to decrypt the communications and that the messages sent makes sense, both parties can be sure of the safety of their communication. A different key is always produced when there is a new communication between the receiver and the sender, but confidentiality and authentication of such messages can only be affected if the key ended up in the third party who was not intended to receive such message.

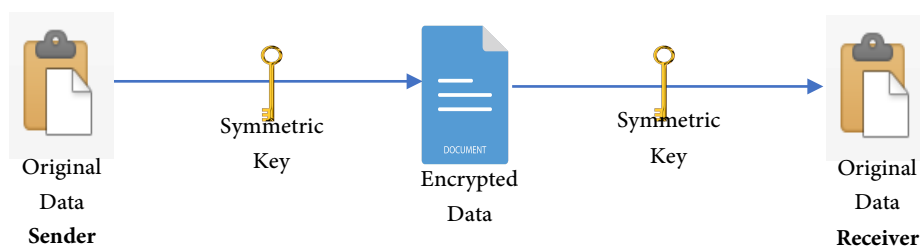


Figure 6.1: Symmetric Key Encryption Process

Types of Symmetric Cryptography

Stream Ciphers

These are ciphers which are mainly used in symmetric key cryptography hence have symmetric algorithms which are used for encrypt and decrypting data.

Advantages

Operates faster than public key cryptosystem with 1000 times speed

Implementation is Simpler and easy to do

Simpler and easier to implement

Used in bulk encryption documentation

Examples of Symmetric Key Algorithms

Twofish, Blowfish, IDEA, Serpent, AES, CAST5, RC4, 3DES, DES, Skipjack, and kuznyechick

6.6.2 Asymmetric Cryptography

This is another form of encryption which uses two keys to encrypt and decrypt sent information and received communication. In most cases these keys can be used either in different cryptographic stages, that is encrypting or decrypting, for example; if key X is used to encrypt, Key W can be used to decrypt and if key W will be used for encryption, key X will be used to decrypt the message. This type of encryption at times it is referred to as public key cryptography because its users at times create another key matching it and make the other key private and give the other key to the public. Private keys can be used to sign messages through encryption, this is very important because the receiver can identify and verify both keys used for encryption and decryption process hence prove the senders secret key is the one that was used to encrypt the message.

CHAPTER 7

SECURITY

WEB SECURITY

There are more than a million web transactions that are being processed each and every day, emails, online shopping transactions, web conferences are transactions done over the internet and need to be secure from malicious attacks. Encryption is the solution to attackers who eavesdrop using stolen physical addresses. Cryptography can be used to securely access systems and sign digital messages.

- Authentication

A participant in a web transaction can be easily identified through the use of digital signatures and also identify participants (receivers) and author of a mail message. The designer or author of such a message can be identified by using digital signatures which can be used together with biometrics and passwords.

- Authorization

To identify the participant in a transaction, authentication is used to determine the authorization of such a participant in such a transaction. Cryptography can be used in distributing a list of users who are authorized in a transaction.

- Confidentiality

Cryptography uses encryption to scramble sent information stored on servers and sent through the networks to prevent eavesdropping attackers to access the contents of the data.

- Integrity

They are methods which are used by cryptography to prevent modification of data during data transition, these are done by using digitally signed message digest codes.

- Nonrepudiation

Receipts are generated to identify the real author of the message lest they deny.

7.1 ATTACKS THAT CRYPTOGRAPHY DEALS WITH

Cryptography ensures a secure computer system will be able to assure the user or the client of Integrity, Confidentiality, Availability, Authentic and Non-repudiation of data during storage and transition, when correctly implemented. Senders and recipients are authenticating each other hence being protected against data repudiation. Communication that is done through untrusted networks like client / server communication, communication done over the internet or private networks can be an advantage to malicious hackers or attackers, but with this type of cryptography, it will be secure. Attacks like passive attacks which attack the network by listening on the communications as it passes through the communication channel are very dangerous since they can be online or offline. SSL/TLS ensures secure systems by providing confidentiality and integrity by not allowing malicious data tampering and eavesdropping. Authenticity ensures that users computer communication is secure and that communication is going on well as intended. Data or information being sent can be assured of its deliverance by preventing disclosure of data which is sensitive, removable devices can be encrypted also to prevent the modification or stolen or loss of data. Integrity is also assured to prevent tempering of data maliciously.

Methods Used for Protecting the Keys

- Keys should be stored in a filesystem secure by a strong ACLs (Access Control List).
- DEKs (Data Encryption Keys) should be encrypted with a second KEK (Key Encryption Key) generated through using the PBE (Password Based Encryption).
- HSM (Hardware Security Module) should be used to store encryption and decryption keys since it is temper resistance appliance.
- Algorithms and key strength should always be used according to the industry security regulations.

7.2 GUIDELINES – NETWORK SECURITY

We can consider the following as a way of preventing network vulnerabilities discussed;

- **Configuration of Firewall:** The main purpose of firewalls is to restrict access which is unwanted to and from the computer systems and from the host controllers implemented, this will improve the responsiveness and the safety of the system hence eliminating unwanted traffic from the network which is unnecessary. Firewall configurations will allow the rules be created specifically for HTTP, DNS, Telnet, TFTP or FTP, SCADA, SMTP, SNMP and DCOM and other industrial protocols. In configuring firewall, things like prevention of Middle in the middle attack, redundancy, single points of failure, fault tolerance, remote access and multicast traffic should be looked into. Basic configuration with rules like *all communications except those communications which are marked to be known and accepted should be denied, Inspection data can be used to monitor the connections which are active and can also be used to on the authorization of packages, Destination IP Addresses and its source should be specified* and lastly *inspection on deep packets should be used to monitor the traffic communication content*.
- **Audit – Network Security:** A security audit should be done to determine the safety of the mechanisms deployed or implemented in the organizations system. They also have the ability of evaluating the systems compliance in the newly established procedures and policies, to determine if they are suitable. There should be an analysis done in the strengths and the weakness of the system and recommendations should be made at the end, if there are any changes found in the policies and procedures set and in the security rules set. Doing an audit, the auditor will need the following;
 - i. List of software's, hardware's, security measures set, services and the architecture of the network which were implemented.
 - ii. A need for a review and a need to make an assessment.
 - iii. Packages of sent and received - logs.

- iv. Applications, services devices and applications, its access mode should be analyzed together with the security measures implemented.
- v. What will backup, implementation and backups procedure be.
- vi. The efficiency of the firewalls with rules should be implemented.
 - **Procedures and Policies:** for a secure system, policies and procedures should be introduced to employees before they can be deployed and implemented for awareness purposes. This will allow the policies to be effective since they are practical and applicable hence productive since there is awareness already. Administrators should be given the rights to authorize and manage these set policies. The policies should follow the following structure;
 1. Define the aims, the scope and the duration of the policy.
 2. Define the responsibility of the users and roles – security.
 3. Making a list of all devices and its individual functionality and all the installed software's in the system.
 4. Defining the rules of the developers, network architecture and the firewalls used.
 5. Listing all the roles, users and the access privileges.
 6. Prevention plan and the vulnerabilities should be described.
 7. Defining the plan for updating the software's and the hardware used.
 8. Describe and define the recovery and backup plans.
 9. Plan for safety training should be defined.
 - **Prevention of Malwares:** Viruses, Trojans horses, adware and spywares and worms are categorized as malwares. To counteract the malwares, packages of Antimalware are used to analyze files stored in the storage devices hence make a comparison between them and the inventory of the files of malwares signatures that seem to be known. Anti-malwares can be deployed either on servers, handheld devices, workstations or even on firewalls. For anti-malwares to work properly there should be compatibility checks done, or there should be a change in management or even in the impact of the performance of the metrics. The systems real-time performance must be considered least it gets compromised due to the implementation of the anti-malwares.

- **Monitoring of Computer Systems Networks:** weak points in the systems are the most vulnerable once hence it gets attacked easily by attackers who wants to access information or data through the network from the compromised system. To monitor the networks, for easy detection of abuse or abnormal operations in the system, Intrusion Detection Systems are used. To determine if there is an attack, a comparison between the network connect and the attacker's database signature should be done, then there should be comparison between other networks to determine if there is an abnormality in their network segments. During this process, it should be clear on which network patterns to monitor, to compare and analyze its logs and from the results make a decision based on the results, by just following the following rules

- All the datagrams of the network protocols of the system with different or wrong length or size should be blocked.
- All incoming and outgoing network traffic to or from an unauthorized area or location should be blocked.
- Packages of the system network protocols should be blocked if they are detected or found in locations they are unauthorized to be or to come from, should also be blocked.
- There should be alerts triggered if there is an attempt of accessing information unauthorized, or if there is any abnormal behavior from a certain application or software.

- **Secure Communications and Access Control:** Authorization and Authentication of policies are part of access control which are set to control and manage the security of accessing the system remotely and the accessing of the network. These two access control mechanisms protect applications and the system by verifying the user's identity – authentication and by authorizing by giving the applications and devices permission to have access. A device attempting to access the system should be identified together with its mode it is using to access the system together with its origin, by filtering ports used, its users, its

applications and by using the principles set like privileges which are least having connections which are limited towards the system. A virtual private network can be used to secure network traffic between network end points hence preventing information or data from being captured. Data that is being transmitted in the network should be encrypted to secure it. Information can also be secured by using protocols which are secure like SFTP or SSH.

- **Architecture of a Network:** Separation of the organizations network and the industrial network should be implemented in order to improve the security of the computer system by using different network configurations. This will help in the implementation of more than one firewall and also in the assistance of creating an isolated area (demilitarized zone) which is used to correspond or correlate to the private network which is found between the organizational network and the industrial network. When the network is properly or correctly configured the demilitarized zone will make sure users which are external do not access the computer system directly hence providing or giving a highly secure system with the ability to filter and control the contents accessed. For the security to be accepted as a solution, there should be two or more areas with separate firewalls being implemented hence they should be carefully deployed.

7.3 BASIC WAYS OF PREVENTING NETWORK ATTACKS

If the organization do not want to be a victim of security network attacks, they can just consider the following points:

- a) Employees should be trained in cyber security aspects concerning the network
- b) Every computer should have antimalware's or antivirus installed in their system and up to date.
- c) All internet connections should have firewall installed.
- d) Operating systems should be up to date with the current updates and patches.
- e) Data should always be backed up and stored out of the network.
- f) Physical and remote access should always be monitored and controlled.
- g) Wi-Fi networks could at all times be secured.
- h) Every employee should have a user account.

- i) Limit installation of software's by users.
- j) Also, limit access of data or information by the users or employees
- k) Passwords should be regularly changed.

CHAPTER 8

ETHICAL HACKING

Understanding What is Hacking

Hacking is a process of accessing a computer system without permission or authorization to do so, this can include viewing files, information, webpages stored in the system or gaining the computer system access without being authorized to do so. Hackers use this process for good will by finding the entry points which exist which can be used for exploitation by dangerous hackers either in the network or the computer system. It can be used to recover passwords which were lost, recover information which was destroyed unintentionally, to strengthen the security in the system or in the network, to prevent breaches which are security related by implementing preventative measures which are adequate and lastly to protect the computer system from unauthorized access. Hacking on its own can also be dangerous if it is done with the intent to harm the system. Tools mainly used for hacking are;

- Nmap
- Owasp
- Command prompt
- Multllidae
- Wamp server

There are three exploitation phases of hacking, the following is the techniques which they use for exploiting the system;

- Networks Attacks
- Spoofing
- WLAN
- ARP Poisoning
- Firewall Traversal
- Man in the Middle attack
- Webservers Attacks
- Code injection
- Session hijacking
- SQL injection
- Cross site Scripting

- Directory traversal
- Services Attacks
- Buffers overflows
- Sessions

The following are the kinds or ways of hacking that hackers uses to get information unauthorized;

Hacking Kinds

- Computer system Hacking
- Email hacking
- Hacking the Web application
- Hacking the Server

Types of Hackers

- Grey Hat Hackers

They get in to the system without authorization, but their intent is to read and see the information without stealing it. Their advantage is that they can report what they have found in the system to the system administrators. Mostly they do this for fun.

- White Hat Hackers

They are hackers who authorized to access the system to find the systems security vulnerabilities hence report them to the system security administrators.

- Black Hat Hackers

These are hackers that get access into the system without being permitted to do so, and their main goal to hack is for their personal benefits, like password, information and money stealing.

UNDERSTANDING PEN TESTING

Penetration testing is a process of identifying any security vulnerabilities in any system or in a software or an application through system evaluation or in the network using different malicious techniques. Weak points within the system are identified and exploited within the testing process by attacking the system through simulated authorized attack. The main purpose of this process is to make sure that data is secure from hackers who unauthorized attempt to access the system remotely. When the vulnerability is being identified, it will be used by the tester to exploit the system being tested for them to gain access into the sensitive important data or information of the organization. A pen testing is used to examine if the set security measures on the system are secure enough in preventing security attacks, it also helps in giving suggestions in solutions to the problems encountered during testing and how they can be reduced and to prevent hackers for attacking the system.

7.4 THE IMPORTANCE OF PEN TESTING

With the forever eruption of ransomwares, viruses and other malicious acts on the systems, it is very important for pen testing to be done frequently on the systems in order to protect the organizations vital information against unauthorized access. Pen testing is done across organizations because of the following reasons;

- To make sure information is secure
- To find loophole is the whole system
- To secure information or data being transferred within the network or between different networks
- To determine security vulnerabilities within an application.
- To determine if there can be successful attacks by the attacker.
- To comply with the security policies set within the organization network infrastructure.
- For better implementation of security measures.

The following aspects should be tested during pen testing to ensure the safety of the organization system;

1. Network
2. Behavior - End-user
3. Operating systems

4. Applications
5. Hardware's
6. Services
7. Processes

7.5 PEN TESTING TYPES

3. Web Application Pen Testing

4. Social Engineering Testing

Various attempts are made towards the systems users to pursue them to reveal their personal information like usernames, passwords and other information that is sensitive. In most cases, they are done through phoning a person or through the internet but targeting a certain group of people like receptionists because in most cases they deal with giving people information about the organization or through the internet, they became the most vulnerable security point.

5. Physical Pen Testing

Data that is seen as sensitive is protected through the use of strong security measures. Network devices and other access points are tested physically for the possibilities of security vulnerabilities or attacks.

6. Network Service Testing

This type of tests is done either remotely or locally to check if there any security vulnerabilities that can be found in the network.

7. Client Side testing

Done in the client side in the software's to find vulnerabilities in them.

8. Remote Dialup war dial

This is done where there are modems by trying passwords to access the internet or by using the brute force.

9. Wireless security testing

Open networks, unsecure hotspots are used for connection purposes hence becomes a great threat to the system.

From the above list, I will discuss web application testing in detail since it is the one which is the door for attackers. The vulnerability of a computer system can be identified by doing a web application pen testing or by testing the network.

7.6 WEB APPLICATION PEN TESTING:

it is used to check the vulnerability of the web applications and the software's in the concerned organizational system. Most of the people have a kin interest in learning how to do *bug bounty* which is an incentive offered to people who report bugs related to vulnerabilities and exploits in websites and software's. But to web penetration tester or network security administrators it is a thing to do time and again to prevent threats and attacks in the network systems by using tools *like burp suite*.

7.6.1 Burp Suite

Burp Suite is one of those integrated platforms which is used for testing the security of web applications, it allows the interception of data which is being sent between the web application and the browser used. It also helps in making the web penetration testers or the network security administrator to understand the transfer of data and how data can be manipulated between the web application and the client / system user. It has various tools which are used during the whole pen testing process, starting with the initial mapping and its analysis of the application surface in attack, through the other step of finding and at the same time exploiting different security vulnerabilities. The main components to consider are, Proxy, the Scanner, a Repeater, a Spider and a sequencer.

To demonstrate this, we will look at the web attacks using the logs and burp suite

Example: I will be testing my MacBook Pro to test it if it is vulnerable to threats and attacks using Firefox browser.

- 3 Set up the proxy: it will allow us to intercept the data being sent
 - a) Open Firefox browser

- b) Go to preferences
- c) Go to the network proxy then open the Settings tab
- d) Select Manual Proxy Configuration
 - Select Use this proxy server for all protocols

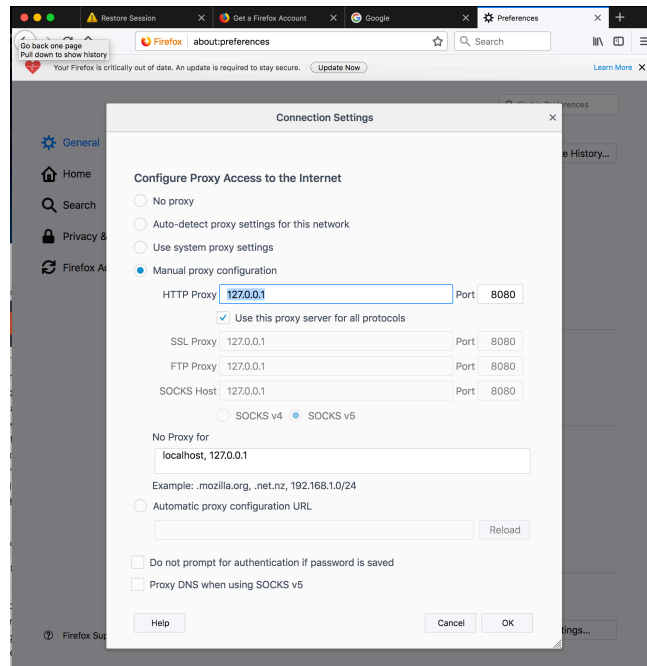


Figure 8.1 Burp Connection Settings

- Then press ok

Open the Burp Suite if installed, if not Download and install it

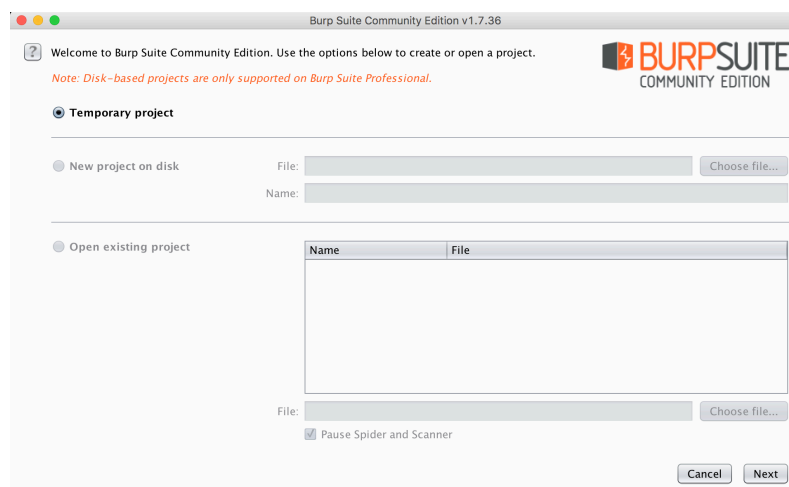


Figure 8.2 Burp welcome screen

- Then press Next
- Leave the option in defaults as they are then press *Start Burp*
- Select proxy Tab then turn Interception *Off*
- Open the Option tab then make sure that the Proxy Listens are the ones you set in Firefox
- Then go to Firefox and search for any text maybe *example.com*, the browser will give an error message then check Burp Suite to see if traffic is recorded.

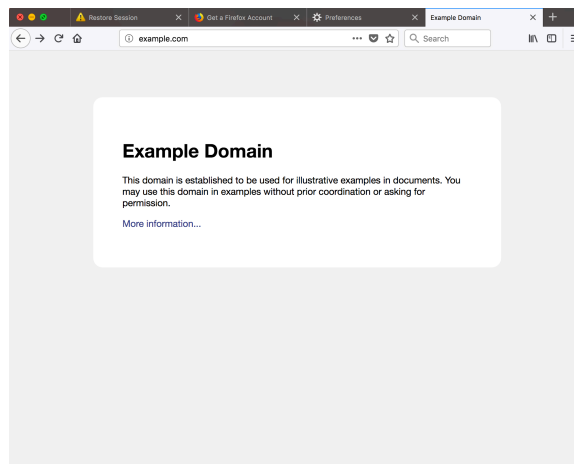


Figure 8.3 Burp Traffic Recordings

 A screenshot of the Burp Suite Community Edition v1.7.36 interface. The 'HTTP history' tab is selected, showing a list of intercepted HTTP requests. The table has columns for #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title, Comment, SSL, IP, Cookies, Time, and Listener port. The first 20 requests are all GET requests to 'http://detectportal.firefox.com' with status 200. The 21st request is a GET to 'http://detectportal.firefox.com' with status 200. Below the table, the 'Request' tab is selected, showing the raw HTTP request details.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
1	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.74	14:44:29 7 Apr 2019	8080	
2	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.74	14:47:27 7 Apr 2019	8080	
3	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	14:53:08 7 Apr 2019	8080	
4	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	14:53:14 7 Apr 2019	8080	
5	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	14:53:15 7 Apr 2019	8080	
6	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	14:53:16 7 Apr 2019	8080	
7	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	14:53:27 7 Apr 2019	8080	
8	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	14:53:29 7 Apr 2019	8080	
9	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:00:35 7 Apr 2019	8080	
10	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:01:15 7 Apr 2019	8080	
11	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:03:25 7 Apr 2019	8080	
12	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:06:57 7 Apr 2019	8080	
13	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:07:20 7 Apr 2019	8080	
14	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:07:23 7 Apr 2019	8080	
15	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:07:25 7 Apr 2019	8080	
16	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.82	15:11:20 7 Apr 2019	8080	
17	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.74	15:15:25 7 Apr 2019	8080	
18	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.74	15:31:25 7 Apr 2019	8080	
19	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.74	15:45:17 7 Apr 2019	8080	
20	http://detectportal...	GET	/success.txt			200	379	text	txt				41.191.219.74	15:45:22 7 Apr 2019	8080	

```

GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
  
```

Figure 8.4 Burp Proxy logs

- IN Bump Suite, I used the example.com domain and it gave me some information like which request was sent to the web application and it also gave me the accept language, accept encoding, the host and the user. The headers will show details like the method used, the host and the agent, all the information similar to the Raw information tab.

Let us try to intercept the information on one of the websites that I am managing www.kanye.adventist.org as an example.

- Let Interception be *ON*, on Burp Suite and open the webpage to see the results (by default the website will state that the connection is not secure, add that as an exception).
- The following shows a success to intercept with one of the websites am managing.

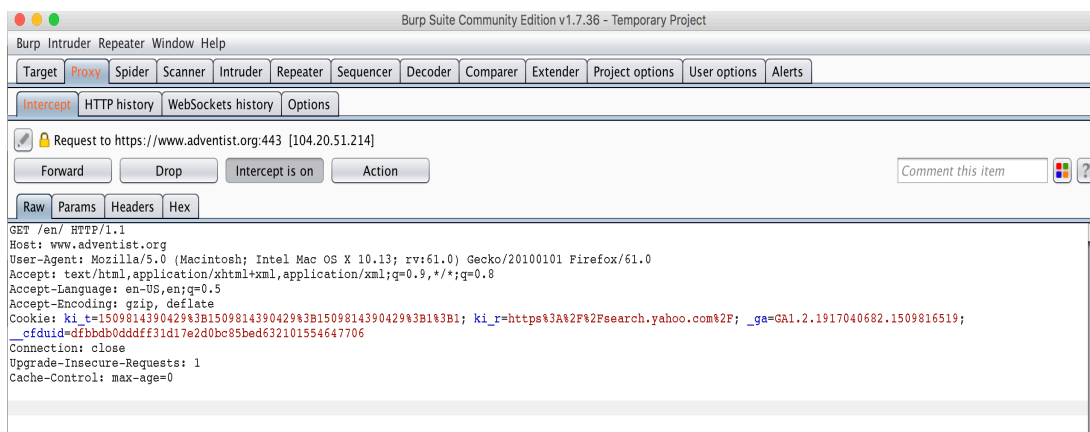


Fig 8.5 Burp Interception requests

Here you have to press forward tad to forward the request so that the website can be intercepted

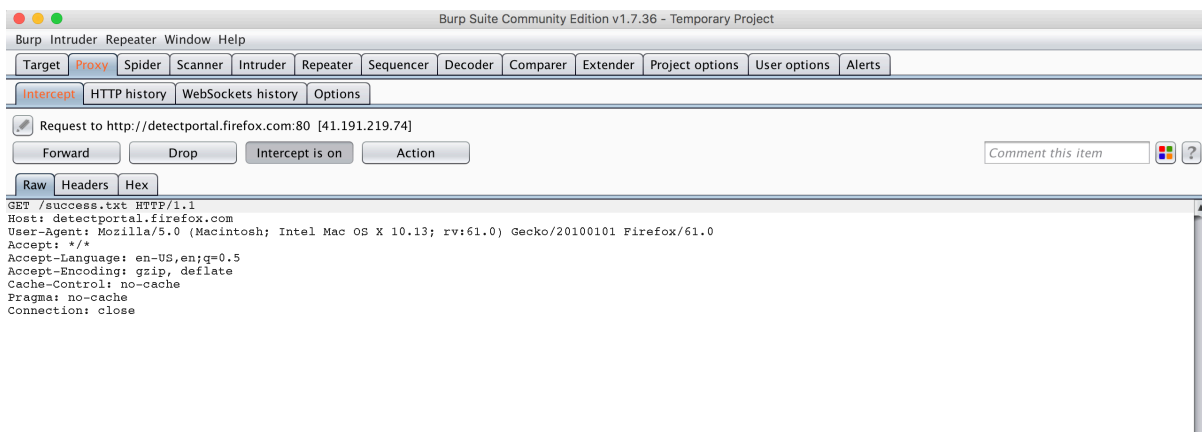


Fig 8.6 Burp Interception Results

This is a screen that shows that the website has been successfully being intercepted and will show all the data that has been sent by the client to the web application. In this stage the data can be analyzed and be further manipulated to find any vulnerabilities within the web application.

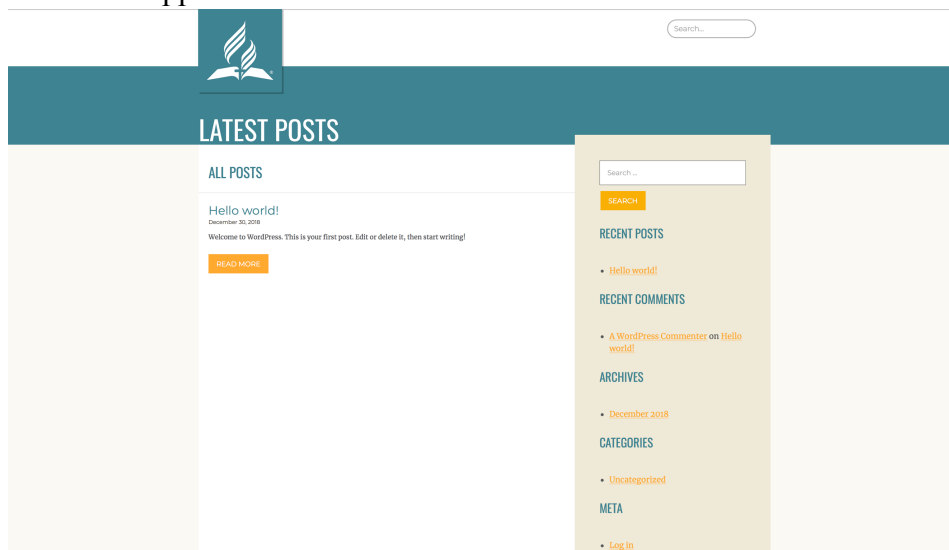


Fig 8.7 Burp Interception website

7.6.2 TECHNIQUES – PENETRATION TESTING

1. Manual test
2. Automated test tools
3. Combination of Manual and Automated

7.6.3 STANDARDS - PEN TESTING

1. PCI DSS
2. ISO/IEC 27002, OSSTMM
3. OWASP

SPIDERING AND DVWA

It helps the penetration tester to identify the scope of what they really want to scan or test by mapping out the web application through finding web forms and links, since it will allow the attacking and manipulation of web forms and headers and others.

Damn Vulnerable Web Application – DVWA

This is a tool that is used for testing the vulnerability of a web application which is PHP/MySQL based web application which is vulnerable. It is an aid to security professionals who use it to test their tools, skills and their web applications in their work area or their organizations or environments which are legal. DVWA helps web developers to easily understand the way they can use to secure the web applications as they use develop them. This will help the concerned parties to know the vulnerabilities of the web which are common and the levels in which the threats and attacks can be in.

RECOMMENDATIONS AND FUTURE WORK

On this research, there were different approaches made in this thesis which worked together to give an understanding to the research question; *What are the other measures that can be used to prevent network cyber-attacks in organizations and in individual network?*, for easy understanding of this question, the research topic was divided into three sections which address the different views of dealing with this problem, by addressing what is *network cyber-attacks*, *ethical hacking* and *network security*.

The results gathered from this research was that cyber-attacks comes as a result from the way people behave when they are in the internet, how they operate on the work environment and the level of understanding the attacks or threats in the cyber world. There has been discovered that there are more people who are engaged in a day to day work over the internet with over more than a million unprotected devices connected to the network and communicating over the internet.

During an observation, it has been observed that people are victims of phishing scams since they are not aware and what they do is just to copy and paste what is available to them, (Andrew, H. 2016). This has become a major threat because there are more readily available tools that people who want to engage in illegal activities use to attack or commit crime. Though ethical hacking was developed to help to curb the growing situation, we might not as well not keep a blind eye to those individuals who use it to commit crime by attacking organizational computer systems since these tools are an open source and are free online. However, there are developments and expansion in the software's used for ethical hacking as a solution to increasing cyber-attacks problems, with more courses that are free online to allow organizations and experts to be prepared for such attacks. But with the effort that OWASP offers, by developing and providing software security tools which are visible through the sharing of devices in a network, cyber world can be a better place to work from. We can come to a conclusion that, the resources should be placed in a central location for the improvement of ethical hacker's performance since the future of the ethical hackers' performance is based on them, if there is a decline in them their performance will also be affected hence the increase in network cyber-attacks.

9.2 Future Work

Future studies into this research object is recommended where can concentrate on the behavior of people on accessing resources online. This is the most important part of the research problem hence more further research in essential. Doing a survey will not be necessary when looking at the behavior of people with a likelihood of not being honest, if they are asked questioned about how they behave online. A more detailed research can be done if the concentration is based on the resources that are paid and not paid to balance the research since most of the hackers use resources that are paid.

Recommendations

Open Source Hacking Resources

These are recommendations and suggestions regarding the hacking resources;

- Free resource offering companies such Kali –Linux which offer offensive security services for free hacking activities, should be advised to add features that will track their downloads, such as registering the downloads and keeping track through IP addresses of where they are used.
- Hacking courses that area online should be not left open for everyone to access them but they should be protected but allowing people to register for them.
- IP addresses for devices that will be used to attack should be provided, where they will be asked to confirm its them who requested for such an action, therefore any action that cannot be traced should be taken as a malicious attack and legal actions be taken upon them.

These recommendations can be used to help reduce illegal usage of these free resources which its main intention is to be used for good purposes.

Peoples Attitude or Behavior to Cyber-attacks

There are ways that can be used to deal with the people's attitude toward committing cyberattacks which are;

- Governments can make cyberattacks awareness programs for its people which can be accessed anytime in platforms like Radios, Internet

through the use of adverts, TVs and posters, which can motivate people by including things like interviewing victims of cyber-attacks or through the use of case-studies to sensitize people.

- People who commit such crimes should take responsibility for their actions by facing the wrath of the law which include restricting them from accessing the computers or any device that connect to the internet or punishing them by working without being paid for the organization they attacked.
- Parents should be educated on such an area so that can be able to make their kids aware of the danger of certain cyber activities that can lead to cyber-attacks and how they can behave themselves when they are transacting online. Dangerous activities like script kiddies and cyberbullying.
- Organizations must be punished also for not protecting the network infrastructure.

Future Research

For the coming researches on this topic, there are a number of suggestions that can be considered which are possible;

- There can be redeployment of the survey with a selective option like types of audiences which can include law makers, IT professionals with experience with no information on cyberattacks and students studying this area.
- A different research survey can be done with can be broader by including broader tools used in ethical hacking.

Conclusion

This thesis has given highlights on the network and the internet with the current environment and the behavior of users in the internet and in the work place as a major contribution to an increase in network cyber-attacks that are leaving companies helpless. A lot of people are engaged in online activities on daily bases which increase the crimes committed online. Above are a number of solutions that are possible which have been suggested and recommended as a solution to the attacks made in the networks. With the increase of online

hacking courses, hacking tools and the level of computer understanding, with an increase on cyber-attacks, further research can be done.

REFERENCES

Georgia, W. (2014), *Penetration Testing: A hands-on introduction to Hacking*, no starch press, San Francisco.

Reckless, W. (1973), *The Crime Problem, 5th Ed*, Englewood Cliffs, NJ: Prentice- Hall.

Prendergras, S. (2013), *What is Anonymous? A Case Study of an Information Systems Hacker Activist Collective Movement*, Diss. Robert Morris University.

Prewitt, F., & Callahan, M. (2017). *Jurisdiction in the Information Age*. In I. I Robert Morris University.

David, K & Patrick, E. (2011), *The basics of Hacking and Penetration Testing; Ethical hacking and penetration Testing Made easy, 2nd ed*, Syngress, Wyman street.

Rogers, M. K. (2006). A Two-Dimensional Circumflex Approach to the Development of a Hacker Taxonomy. *Digital Investigation*

Hart, C. (2011), *Mobilizing the Cyberspace Race: The Securitization of the Internet and its Implications for Civil Liberties*, Cyber-Surveillance in Everyday Life: An International Workshop, University of Toronto

Rogers, M. K. (2011). The Psyche of Cybercriminals: A Psycho-Social Perspective, *Cybercrimes: A Mutlidisciplinary Analysis*, Berlin Heidelberg: Springer.

Hare, F. (2010), *The Cyber Threat to National Securirty: why can't we agree?*, *Conference on cyber Conflict*, Proceedings 2010.

Taylor, H. (2017). Retrieved from Krebs on Security: <https://krebsonsecurity.com/wp-content/uploads/2017/04/W.D>

Buzan, B. & Hansen, L. (2009), *The evolution of International Security Studies*, Cambridge University Press, Cambridge

Spears, R., Reicher, S. D., & Postmes, T. (1995). A Social Idenetity Model of Deindividuation. *European Review of Social Psychology*.

Nissenbaum, H. (2005), *Where Computer Security Meets National Security, Ethics and Information Technology*, Vol 7, No. 2

Andrew, W & Daniel, N (2006), *Security, Penetration Testing and Network Defence, the practical guide to simulating, detecting, and responding to network attacks*, Cisco Press, Indianapolis

RAND Corporation. (2016). *The Role of the 'Dark Web' in the Trade of Illicit Drugs*, Retrieved March 28, 2019, from http://www.rand.org/pubs/research_briefs/RB9925.html

Eriksson, J. & Giacomello, G. (2006), *The information Revolution, Security and International Relations: (IR) Relevant Theory?* International Political Science Review Vol. 27:221-244

Waite, E., Rossi, Berk, R., & Bose, C. (1974). The Seriousness of Crimes: Normative Structure and Individual Differences. *American Sociological Review*.

Education, (2016), *Intellectual Property Law 2017 Edition, Global Economic Crime Survey*.

Raymond, E. (1996). *The New Hacker's Dictionary*. MIT Press. Reckless, W. C. (1961). A New Theory of Delinquency and Crime. *Federal Probation*

Udris, R. (2014). Cyberbullying Among High School Students in Japan: Development and Validation of the Online Disinhibition Scale. *Computers in Human Behaviour*.

Vipin, k., Jaideep, S & Aleksandar, L (2005), *Massive Computing, Managing Cyber Threats, Issues, Approaches, and Challenges*, Springer Science+Business Media inc, Spring Street.

Raconteur. (2017). *WannaCry: The Biggest Ransomware Attack in History*. Retrieved April 25, 2019, from <https://www.raconteur.net/infographics/wannacry>

Sumedt,J, How to hack a website with Metasploit

Tsai, Lin, S., & Tsai, M. (2001). Developing an Internet Attitude Scale for High School Students. *Computers and Education*.

Dunn, M. (2003), Securing the digital Age: *In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New York: The New Press.

Computer science and telecommunications Board (2002), *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, Washington, Dc: National Academy Press

Thompson, E., & Dodder, R., (1983). Juvenile Delinquency Explained? A Test of Containment Theory. *Youth & Society*.

Zlomislic, V., Fertalj, K., & Sruk, V. (2014) Denial of Service Attacks: An Overview of *Information Systems and Technologies*

ZD Net. (2017) *Six Quick facts to know about the Petya Global Ransomware Attack*, from ZD Net://www.zdnet.com/articles/six-quick-facts-june-global-ransomware-cyberattack/

Briggs, R. O., Reinig, B. & Nunamaker, J. (1998), Flaming in the Electronic Classroom. *Journal of Personlity and Social Psychology*

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention, *International Management Review*.

APPENDICES

QUESTIONNAIRE

These are questions which were used at the beginning of the survey to get the answers from the people and to determine if this research is necessary.

1. What do you work as?
 - a. Information technology personnel
 - b. Secretary
 - c. Human resource personnel
 - d. An officer
 - e. others
2. Do you use internet?
 - a. Yes, I use it
 - b. No, I don't use it
3. How often do you connect to the internet?
 - a. Every 30 Minutes, Every day
 - b. Every hour, Every day
 - c. Every week
 - d. I don't know but I do connect when I feel like
 - e. I don't use Internet
4. Do you have a device that connect to an internet?
 - a. Yes, I have it
 - b. No, I don't have it
 - c. I use a computer at work
5. Are working for a certain organization?
 - a. Yes
 - b. No
6. Is the Company you are working for has a network?
 - a. Yes, it has
 - b. No, it does not have
7. Does your Organization has an IT Personnel?
 - a. Yes
 - b. No

8. What is your position in the organization?
 - a. Full time Employee
 - b. Part time Employee
9. Does your job require you to use network or internet every-day?
 - a. Yes
 - b. No
10. How often are your services need as the IT specialist or Expert?
 - a. Every day
 - b. Twice a day
 - c. Almost every time
 - d. Never
11. Do you have a security personnel's or team in your organization?
 - a. Yes
 - b. No
 - c. I don't know
12. Are you able to identify a computer which is infected with virus?
 - a. Yes
 - b. No
13. Does your company has a contact person in-case of computers being hacked or infected?
 - a. Yes, they have
 - b. No, they outsource
 - c. We don't notice anything, unless the computer switch its self-off.
14. Have you experienced an infected computer in your organization?
 - a. Yes
 - b. No
 - c. I don't know when a computer is infected
15. Can you tell if your computer is attacked by a Trojan?
 - a. Yes
 - b. No
 - c. What is a Trojan?
16. Have you ever received an email asking for your login credentials (username and Password), and you provided them?
 - a. Yes, I did receive and provided them
 - b. Yes, I did receive and did not provide them

- c. No, I did not receive.
17. How secure do you think your computer is?
- a. Highly secure
 - b. Just secure
 - c. Not secure at all
 - d. I don't know
18. Do you have a firewall in your network?
- a. Yes
 - b. No
 - c. I don't know
 - d. What is a firewall?
19. How often do your computers gets software updates?
- a. Automatically, as long as they are available
 - b. Manually, being installed by an IT person
 - c. I don't know
 - d. What are software updates?
20. How do you open a mail with an attachment?
- a. I just download and open
 - b. As long as I know where the email comes from I just open
 - c. I scan the email with the antivirus before I open it
 - d. Is there a problem with opening an email sent to me?
21. Do you know what a network attack is?
- a. Yes
 - b. No
22. Do you know what phishing is?
- a. Yes
 - b. No
23. Do you know an email scam?
- a. Yes
 - b. No
24. Does the computer you are using have an antivirus which is enabled and upto date?
- a. Yes
 - b. No
 - c. I really don't know

- d. What is an antivirus?
- 25. The organization am working for is not a target to attackers since it does not make a lot of money.
 - a. True
 - b. False
- 26. Does our website have policies that describe how to take care of ourselves in the internet?
 - a. Yes, they are very helpful
 - b. Yes, there are there and I don't have time to read them.
 - c. No, we don't need that
 - d. I don't know
- 27. Does your organization allow instant messages?
 - a. Yes
 - b. No
 - c. Have not seen that
- 28. Does your organization allow workers to use their devices at work?
 - a. Yes
 - b. No
 - c. Why not
- 29. Are all workers allowed to access the organizational information?
 - a. Yes
 - b. No
- 30. Have you downloaded any software into your work computer?
 - a. Yes
 - b. No
- 31. Have you disclosed your computer or email password to your work colleagues?
 - a. Yes
 - b. No
- 32. The password that you use, is it used only for work logins or do you use it in other accounts like personal facebook, email, twitter and others?
 - a. Yes, so that I don't forget it
 - b. No
- 33. How often do you take work form office to work?
 - a. Everyday
 - b. When I need to

- c. I don't
34. Have you accessed your work computers from a remote location, maybe at home or internet-café.
- a. Yes, I do that a lot
 - b. No, I wish I knew how
 - c. No, I don't do that
35. When was the last time your organizational computers were scanned of viruses?
- a. Every 6 months
 - b. Every year
 - c. It has been a long time
 - d. No, we just use antiviruses
 - e. No, there is no need to scan them
36. Have your company experienced crime committed by a computer?
- a. Yes
 - b. No
 - c. We usually have cases that we don't know how deal with them since there is no evidence.
37. Define network cyber-attacks according to your understanding.

Comments of Respondents

Since the questionnaire did not request long answers just to select a lot of participants showed they were clueless in attacks done over the network, the reason could be that in question 1, 5% of the respondents were the ones who were Information technology experts who knew what network cyber-attacks were, while 95% were clueless in the subject matter. In question 2 most of the respondents said indicated that they use internet in their daily routines while question 3 they stated that they do not have a specific time when they connect to the internet, they just connect when they feel like connecting. 95% said they have their own device that they use to connect to the internet while in question 4 and in question 5, while 100% said they have internet in their organizations and they are free to use it for their personal use for question 6. It is scary to find that 15% of the companies have information technology experts which is a problem since most of the companies do not have people who are responsible for their organizational security (Q.7). Most of the respondents are employed on full time bases constituting to 87% in Q.8 while in Q.9 all the people use internet on their daily work activities. Since we had few IT respondents in this research, they just stated their services are not needed in most cases at work which is being addressed by Q.10. There are no policy or security teams implemented in these organizations, they just depend on the outsourcing IT personals who at times are not trained or do not have an idea on cyber security – Q.11 and Q.13. Since most of the respondents are not aware of threats and attacks, 89% stated that they are not familiar with computers under the strain of malicious acts or infections, Q.12, Q.14 and Q.15. Respondents showed that they are prone to phishing since a higher percentage of them providing their credentials over the email request from unknown emails (Q.16). They indicated that they do not know anything concerning the security of the computers they are using which is being addressed by Q.17. In Q.18 there are firewalls placed in computer systems which others are not active or enabled hence there is no security placed for other systems, since the organizations do not have IT professionals, most of their operating systems are not set to automatically update since they are set to manually, so they end up not being able to see if there are updates for patching the software's (Q.19). There are a lot of malicious codes being spread in organizations systems, since most of the respondents stated that they open the emails without scanning them for malicious codes, (Q.20). Phishing, network-attack and email scam are terms that 75% of respondents do not attempt to answer which stated that they do not understand what it may be reference to while 15% claimed to know the answer

to such questions, (Q.21-23). Computer systems have antiviruses which are not updated so this means systems are prone to malicious activities, Q.24, most organizations are a target to cyber-attacks since the respondents show it not being a target since it does not have what can attract attackers into their company, Q25. 87% do not have policies set on their websites to guide them on how to behave in the internet- Q.26 while 25% of the organizations do accept instant messages-Q.27. Almost all organizations allow their employees to connect into the work network using their own devices such as phones and tablets – 96% - Q.28. There are no measures set aside on how to access the organization information, everyone has access to the information, regardless of their position in the organization, - Q.29. As there are no professionals in these organizations to restrain workers from accessing and installing software's, 69% stated that they do download software's and install them if they want to –Q.30. Q.31 – As workers sometimes need to access other information from other computers in the work environment, instead of them sending emails to those who need that information, they will give them their log in credentials to allow them to access their computers any time they want, with passwords being shared among workers, then applies to same passwords being used across other login different platforms – Q.32. As the pressure increases at the work place 56% of workers admitted to taking their work to their homes and 43% at times access their work network in remote locations like at the internet café's – Q.33 to 34. 45% of organizations depend on identifying viruses by scanning their computers with antiviruses while 7% see no need in scanning for threats, while others (25%) don't remember when it was done, Q.35.

These responds make it a good reason to continue with this research thesis.