UNIVERSITI TEKNIKAL MALAYSIA MELAKA

READINESS LEVEL ON CONDUCTING PENETRATION TESTING AMONG NETWORK ADMINISTRATOR IN KOLEJ POLY-TECH MARA

MIMI DALINA BINTI IBRAHIM

MASTER OF COMPUTER SCIENCE
(INTERNETWORKING TECHNOLOGY)

2016

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Faculty of Information and Communication Technology

THE READINESS LEVEL ON CONDUCTING PENETRATION TESTING AMONG NETWORK ADMIN IN KOLEJ POLY TECH MARA

Mimi Dalina Binti Ibrahim

Master of Computer Science (Internetworking Technology)

2016

READINESS LEVEL ON CONDUCTING PENETRATION TESTING AMONG NETWORK ADMINISTRATOR IN KOLEJ POLY-TECH MARA

MIMI DALINA BINTI IBRAHIM

A report submitted
in fulfillment of the requirements for the degree of Master of Computer Science
(Internetworking Technology)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2016

DECLARATION

I declare that this report entitled The Readiness Level on Conducting Penetration Testing among Network Admin in Kolej Poly Tech MARA is the result of my own research except as cited in the references. The report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……………………………………..

Name : ……………………………………..

Date : …………………………..………

APPROVAL

I hereby declare that I have read this report and in my opinion this report is sufficient in terms of scope and quality as a partial fulfillment of Master of Computer Science (Networking Technology).

Signature : ……………………………..

Supervisor Name : ……………………………..

Date : ………………..…………

DEDICATION

Alhamdulillah

To My Beloved Husband

Mohamad Nasir Bin Ahmad Yusop

To My Beloved Mother

Zainab Binti Abdullah

To My Beloved Supervisors

To My Beloved Brothers and Sisters

To My Beloved Friends

ABSTRACT

Nowadays, most of Malaysian cannot live without internet. Malaysia become one of the country which used internet widely. However, the number of attack, suspicious event and vulnerabilities in internet increases day by day. The network administrator have to observe and monitor the network to find the suspicious event and weakness that may occur in network under their supervision. This research focus to investigate the readiness level on conducting penetration testing among network administrator in Kolej Poly-Tech MARA (KPTM). This research aimed to investigate the factors which may contribute to the readiness on conducting penetration testing among user Information Technology (IT) focus to Network Administrator in Kolej Poly-Tech MARA (KPTM), design and develop a questionnaire that cover about factors which relate to readiness in using penetration testing and analyse the relationship between dependent and independent variable towards readiness level on using penetration testing. The selected factors which are experience, knowledge and organization was explored through literature survey and interviews with IT expert. A total of 22 respondents from different level of network administrator in KPTM around Malaysia are selected for the purpose of this study. For the analysis, one way ANOVA, Pearson Correlation Coefficient and Regression was adopted to analyse the results. The result shown that all the factors have positive linear relationship between organization, experience and knowledge. This study also provides contribution from the study, limitation of the study and recommendations for future research in penetration testing.

ABSTRAK

Pada masa kini, kebanyakkan rakyat Malaysia tidak boleh hidup tanpa rangkaian internet. Malaysia menjadi salah sebuah negara yang menggunakan rangkaian internet dengan sangat meluas. Namun, kadar serangan di dalam rangkaian, perkara-perkara yang mencurigakan dan kelemahan-kelemahan dalam rangkaian internet bertambah hari demi hari. Pentadbir rangkaian perlu memerhati dan memantau rangkaian internet untuk mencari perkara-perkara yang mencurigakan seterusnya mencari kelemahan-kelemahan yang mungkin terjadi dalam rangkaian di bawah seliaan mereka. Kajian ini tertumpu kepada menyiasat kadar kebersediaan pentadbir rangkaian dalam mengendalikan ujian penembusan di Kolej Poly-Tech Mara (KPTM). Kajian ini mesti memenuhi tiga objektif; antaranya menyiasat faktor-faktor yang mungkin menyumbang kepada kebersediaan dalam mengendalikan ujian penembusan dikalangan pengguna teknologi maklumat fokus kepada pentadbir rangkaian di Kolej Poly-Tech MARA (KPTM), merekabentuk dan membangunkan soalan kaji selidik yang meliputi faktor-faktor yang berkait dengan kebersediaan dalam menggunakan ujian penembusan; dan menganalisa serta menilai kadar kebersediaan dalam menggunakan ujian penembusan. Faktor-faktor yang telah dipilih adalah organisasi, pengalaman dan pengetahuan telah diperolehi melalui kajian literatur dan temubual dengan pakar teknologi maklumat yang dipilih. Seramai 22 responden yang terdiri daripada pentadbir rangkaian dari pelbagai tahap di KPTM sekitar Malaysia dipilih bagi tujuan kajian ini. Untuk analisa, ANOVA satu hala, Pekali Korelasi Pearson dan regresi telah diterima pakai untuk menganalisa keputusan. Keputusan kajian menunjukkan bahawa semua factor mempunyai hubungan linear positif antara organisasi, pengalaman dan pengetahuan. Kajian ini turut memberikan sumbangan daripada kajian, batasan kajian dan cadangan kajian lanjutan dalam ujian penembusan.

ACKNOWLEDGEMENTS

In the name of Allah, Most gracious, Most Merciful. All praises belongs to Allah. First of all, I would like to thank to Allah Al the Mighty, who made me capable to complete the report throughout those difficult years.

First and foremost, I would like to thank to my supervisor, Associate Professor Madya Dr. Abdul Samad bin Hasan Basari for his excellent supervision, guidance, supporting and encouragement towards in completing my report. May Allah reward him with a reply that much better than what all he has done.

I am in debt and owe great thanks to my beloved husband (Mohamad Nasir), my mother and my siblings especially my sisters for their patience, inspiration, continuous encouragement and thoughtful advice throughout my years as a Master student.

I would like to extend my thanks to my colleagues, Staff in Department of Information technology and Communication for their time, guidance and support during my study. I would also like to thanks to my employer and sponsor, Majlis Amanah Rakyat (MARA) for their funding support my study. Last but not least, my special thanks to all my friends for their time, understanding, advice and continues moral support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

LIST OF APPENDICES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ANOVA	Analysis Of Variance
CCENT	The Cisco Certified Entry Networking Technician
CCIE	The Cisco Certified Internetwork Expert
CCNA	CISCO Certified Network Associate
CMS	Campus Management Online System.
DFR	Digital Forensic Readiness
HAIS	Human Aspects of Information Security
ICT	Information And Communications Technology
IT	Information Technology
KPTM	Kolej Poly-Tech MARA
NRI	Network Readiness Index
RLPTNA	Readiness Level of Penetration Testing among Network Administrator
SE	Software Engineering
SPSS	Statistical Package for the Social Sciences software

LIST OF SYMBOLS

β	Unstandardized coefficient
C	Constant value
H_0	Hypothesis null
X	Dimension of independent variable.
Y	Prediction relationship of types of variables toward readiness.

CHAPTER 1

INTRODUCTION

- ## 1.0 Introduction

Readiness is one of the important variables investigated in this study and the term is defined by the Oxford Advanced Learner's Dictionary as "The state or quality of being ready; preparation; promptness; aptitude; willingness. Prepared for what one is about to do or experience; equipped or supplied with what is needed for some act or event; prepared for immediate movement or action". As pointed by (Schreurs et al., 2008) readiness also takes account of students' capability to adapt to "…technological challenges, collaborative training and synchronous as well as asynchronous self-paced training".

How to protect our valuable assets? The question is easy to answer; but hard to implement. One of the method is to keep the assets in a safe place like a bank, vault, locked case and others. However, that method is still not safe; because we heard about bank and house robbery with the equipment and technology used to rob. In that case, we supposedly take action to reduce the chance from being rob; for example, make sure that the premise have hired the guard in order to protect the bank from suspicious people which tend to do something bad or we could suggest to the police department to do regular monitoring and place a station to monitor the banks.

This research is about security for the computer-related assets which including the security for computing systems in an organizations. How user of Information Technology (IT) - people and organization do protections? Most of the user IT (network administrator) and organizations recognize computer and their data as a valuable resources where they already applied suitable protection by using suitable tools, hardware, software and procedures. However, computing system part can be attack by a computer crime. We have to identify tools or techniques used to prevent the assets from being rob and attack. In order to protect the computer-related assets from being touched, regular monitoring should be done to check the suspicious event and weaknesses in the network; indirectly protect the web application and system used.

Kolej Poly Tech MARA (KPTM) is a higher institution which own an official website and Campus Management Online System (CMS). Unfortunately, the website and the system have been hacked by attackers. From the observation, it can be concluded that the network admin failed to observe the network to find the suspicious event and weakness of a system earlier. The effect from the attacked cause the users can’t use the website and online system in two weeks where the online registrations for new students can’t be made on the moment the website being hacked. To overcome this problem, a literature survey will be made and an interview session with IT expert will be conducted to find the factors that relate to the readiness level among Network Administrator in Kolej Poly Tech MARA (KPTM). In all organizations, user IT (network administrator) play an important role to protect their network from being attacked and hacked. One of the tools or techniques that they should use is running a penetration testing regularly; in order to check the weaknesses and holes in the network (Hassan et al., 2013). Tools can be used to identify the security risks in the network or information systems. The existence of security risk will lead to potential of threat which can destroy the valuable assets. So, one of the tools that can be used by the network administrator is Penetration Testing (Shi et al., 2010). Nmap, netcat and hping are some of tools in penetration testing which can be used by attackers, user IT and network administrator (IT professional) to get access into the network (Alqahtani and Iftikhar 2013).

By conducting a penetration testing will help the organization to protect their valuable assets from being hacked; defending through financial loss, gain trust from the customers and stakeholders and maintaining corporate image. For government and educational sector, protection of important and confidential information are important to them (Hassan et al., 2013).

- **Research Background**

Computer science is not only about hardware and software for computation. Computer science more than write a program. Computer science have seven subfields which are Artificial Intelligence (AI), Software Engineering (SE), System, Graphic and Multimedia, Programming and Networking (Streubel, 2003). Networking play main components in computer system nowadays; with the potential to exchange the message between two devices through transmission medium. Networking field fall into network programming, neural network and network security (Lu et al., 2013). Recently, many researchers found that network failure always happen in modern industries (S. et al., 2011). The rapid development of computer network technology and the internet technology, people especially network administrator more aware of the needs and significant of network security; and the increasing of attack everyday make the network security became the main issue in computing that should taking care. Security in network divided into attack and defense. When monitoring network, we should find any abnormal activities that occurs in the analysis. Network administrator want the security system protect the data from unauthorized parties (Charles P. Pfleeger. et al. 2003). Attack have three focus which are threat, vulnerabilities and controls. Threat is a potential causes of loss or harm in computing system; vulnerabilities is a weaknesses in a network, web application or system; while controls is a method that used to protect the network. To protect network against harm, a good defense should develop. Defense fall into six categories including controls, encryption, software controls, hardware controls, policies and procedures and physical controls. We are focusing on how to controls the network from being attack. There are many tools that can be used to audit the network or system; including Antivirus, Intrusion Detection System (IDS), Firewall and Penetration Testing.

To estimate the level of risk or harm faced in the network is by using the penetration testing service; where a good planning will produce for counter back the risk (Bassill, 2013). Penetration Testing is a method that network administrator can use to ensure that the suspicious event, vulnerabilities and weaknesses in network can be identified before something terrible happen or exploited in real attack. The result from the test can be used as an evidence or proof of any weaknesses in network (Tang, 2014). The malicious codes, suspicious event and weaknesses are possible create a problem in the network.

There are few factors to be considered which are possible that contribute to readiness evaluation; including organizational factor, individual factor and technological factors. To evaluate the readiness level among network administrator, we will distribute a questionnaire by using quantitative and qualitative approach on selected population which focus to Kolej Poly-Tech MARA (KPTM); because large amounts of information from respondents can be gathered in a time not too long and save money. The analysis and results from the questionnaires can be quickly and easily measured through the use of a software package. When data has been quantified, it can be used to compare and contrast other findings and may be used to measure change. Unfortunately, this approach have some drawback to the findings; which the questionnaire questions is an art by the researcher because the number of questions are limited and there is no way to tell how truthful a respondent has put in. The respondent may forget or not thinking within the full context of the situation and they may understand the questions in different way and therefore reply based on their own interpretation of the question.

According to Shivayogimath (2014), penetration testing become important and play roles to access the network security and check the information system from attacker's view. The penetration tester can determine and address the malicious event and threat if they follow the right methodology. To make sure that the penetration testing is success, (Chu et al., 2011) found the right approaches and method to conduct the testing. The researchers found three phases to run the penetration testing step by step; information gathering, vulnerability analysis and vulnerability exploit. They choose two samples of web applications when conducting the test; resulting user-input and cookies field would possible be the attack. However, Mainka et. al. (2012) develop a general framework and used web services attacker as a penetration tools but that tool can't handle a lot of attacks.

- **Problem Statement**

Nowadays, most of Malaysian cannot live without internet. Malaysia become one of the country which used internet widely. In 2003, a study shown that 67% of Malaysian was using internet in their live (Society, 2014). The vast use of internet caused hackers have the chance and potential to launch the attack. One of the attack that launched on government website in Malaysia – Famous hackers sent alarm threat to Prime Minister and Banks – Malaysian ATMs were hacked of RM3 Million by Latin Americans are some examples showing that hacking is very serious problem for the last decade. It can tell that the hackers try to prove their power in hacking technique. From the observation, the network administrator failed to observe the network to find the suspicious event and weaknesses because some companies are outsourcing the network service, lack of knowledge in monitoring the network and don’t have sufficient equipment and software for monitoring. The attack may harm the company or institute (government, private sector, industries, banking), end users and students in educational institute in their daily activities or work. To overcome this problem, questionnaire will be distributed to investigate the readiness level on conducting penetration testing among Network Administrator.

This study will focus on groups of user IT including IT technician, network administrator, IT Officer and head of IT Officer in KPTM. So, the questionnaire questions conducted is based on some selected factors which effect the readiness.

- **Research Objective**

This research consists of three objectives:

- To investigate the factors which contribute to the readiness level on conducting penetration testing among user IT focus to Network Administrator in KPTM.
- To design and develop a questionnaire that cover factors which relate to readiness in using penetration testing.
- To analyse the relationship between independent variable and dependent variable to seek the readiness level on using penetration testing in KPTM.

In order to fulfil this objectives, the study aims to seek answers to the following research questions (RQ):

RQ 1: What is the factors that contribute to readiness to conduct penetration testing?

RQ 2: What is the reliability and consistency of the construct?

RQ 3: Is there any positive linear relationship between organizations towards readiness on conducting pen-testing?

RQ 4: Is there any positive linear relationship between experience towards readiness on conducting pen-testing?

RQ 5: Is there any positive linear relationship between knowledge towards readiness on conducting pen-testing?

- **Scope**

  - This project will be conducted by using questionnaire method where quantitative and qualitative approach are selected to find the correlation between factors.

  - For this study, a set of questionnaire will be distributed to user IT focus to the network administrator in Kolej Poly-Tech MARA (KPTM). Total of the respondent that will contribute in this survey are around 30 respondents who responsible in monitoring the network.

  - During the phase of data collection, all of the collected data will be analyze using Statistical Package for the Social Sciences (SPSS) software.

Expected Outcomes

A computer system, network and web application can never be completely secure. Through the questionnaire, the gathered data will be analyzed. This research findings are expected to:

- Show a strong readiness to handle any kind of weaknesses and suspicious event by using a penetration testing among network administrator and IT technician.
- Increase the understanding of the importance of penetration testing and the potential risks with insufficient security and protection.
- To show that some of the factors effect their readiness level in penetration testing.
- Improve the understanding of the variety of potential threats that network administrator must aware and the creativity of the attackers.

Fast action could be taken to protect the network from been hacked. Monitoring the network or system should be done regularly to check the abnormal activities (suspicious event, vulnerabilities and weaknesses) in the network. Meaningful result can be produced by the survey analysis

Report Organization

This chapter is a brief description about the research of the readiness level on conducting penetration testing among Network Administrator. Some of the network administrators are new in networking area. This research is focused on the Network Administrator and IT Technician