ANALYSIS OF NETWORK THREATS THAT EFFECT THE BANDWIDTH UTILIZATION IN UniMAP STUDENT CAMPUS

A thesis submitted to the Academic Dean Office in partial
Fulfilment of the requirement for the degree
Master (Information Technolgy)
Universiti Utara Malaysia

By

MOHAMMAD TAUFIK BIN SAIDINA OMAR (800754)

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

MOHAMMAD TAUFIK SAIDINA OMAR
(800754)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

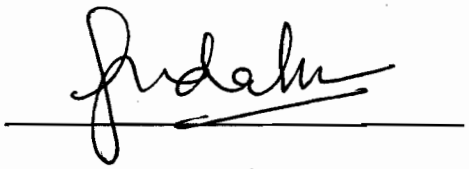
telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

ANALYSIS OF NETWORK THREATS THAT EFFECT THE BANDWIDTH UTILIZATION IN UniMAP STUDENT CAMPUS

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC. PROF. DR. HUDA HJ. IBRAHIM**

Tandatangan
(Signature) : 

Tarikh
(Date) : 19/5/2010

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Academic Office. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of Academic Office
UUM CAS
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRACT

Threats can happen everywhere. Same goes to the IT environment where the networking part is the most critical. It is because; network threats like viruses, spywares and forbidden application are using the network to launch the attack silently. A study has been done in Universiti Malaysia Perlis (UniMAP) where one of the student hostels is identified for the place to do the network analysis. The hostel name is Kolej Kediaman Tan Sri Aishah Ghani (KKG) located in Wang Ulu, Perlis. The students have been complaining that the network quality is going very slow and they cannot access to the internet and the internal application like UniMAP Portal, UniMAP website and email smoothly. To overcome this, a network security appliance is obtained to perform the network traffic analysis in order to identify the type of network activity that has congested the KKG network system. A network policy has been applied to deny any unwanted threats, forbidden application usage and access to the bad host.

ABSTRAK

Ancaman berlaku dimana sahaja. Ini termasuk lah dalam teknologi IT dimana sistem rangkaian adalah yang paling kritikal. Ini kerana, ancaman rangkaian seperti virus, spywares dan aplikasi larangan menggunakan saluran sistem rangkaian untuk melancarkan serangan dengan senyap. Kajian telah dilakukan di Univerisiti Malaysia Perlis (UniMAP) di salah satu kolej kediaman pelajar untuk melakukan analisa ke atas sistem rangkaian disana. Kolej tersebut bernama Kolej Kediaman Tan Sri Aishah Ghani (KKG), terletak di Wang Ulu, Perlis. Para pelajar telah merungut dimana tahap kualiti sistem rangkaian di KKG telah menjadi begitu perlahan dan mereka tidak boleh akses ke internet dan aplikasi dalaman seperti Portal UniMAP, laman web rasmi UniMAP dan email dengan lancar. Bagi mengatasi masalah ini, sistem peranti sekuriti rangkaian akan di pasang untuk melakukan analisa ke atas sistem trafik rangkaian untuk mengenalpasti jenis-jenis aktiviti rangkaian yang telah menyesakkan sistem rangkaian KKG. Polisi sekuriti rangkaian telah dilaksanakan to menyekat sebarang ancaman rangkaian, penggunaan aplikasi rangkaian dan akses ke laman web larangan.

ACKNOWLEDGEMENTS

I would like to thank Allah S.W.T for giving the opportunity and strength to complete this research. Thanks to my family especially my mother, Hayati Bt Ahmad, for giving me the support to take and complete this study. Not to forget, my colleagues who have been with me through out my study in UUM. I also would like to express my deep and sincere gratitude to my supervisor, Assoc. Prof. Dr. Huda Bt Haji Ibrahim. Her wide knowledge and logical way of thinking have been of great value for me. Through this study, I have increased my knowledge in analyzing the network system in UniMAP including the way to handle the network threats by using appropriate network security tools.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter explains the main parts of this study including the background of the study; the objective of the study, the research problem, and the research scope. This chapter also presents a brief description of the methodology being used to conduct this study and the significance of the study.

1.2 Background of Study

University Malaysia Perlis (UniMAP) is one of the local universities in Malaysia that focuses in the engineering and technology field where the vision is to be an internationally competitive academic and research institution. Parallel to the university's vision, an efficient internet connection is very crucial in order to help the students, lecturers, and researchers collect new information as well as share and disseminate it among their communities.

Students at UniMAP are now able to access the library using online services such as IEEE Explore, SpringerLink, ACM Digital Library, ScienceDirect, EBSCOhost and other online services which are available to the students in UniMAP and it is accessible from any location within the university's

The contents of the thesis is for internal user only

REFERENCES

B. Harris, R. H. (1999). "TCP/IP security threats and attack methods." Computer Communications 22(10): 885-897.

bin Ismail, N., M. D. bin Baba, et al. (2002). Network performance analysis on bandwidth utilizations and protocol distributions. Research and Development, 2002. SCOReD 2002. Student Conference on.

C. Huegen (1998), The latest in denial of service attacks: smur®ng, *[online:http://www.quadrunner.com/_chuegen/smurf.txt,December].*

Chess, D. M. (1989). "Computer viruses and related threats to computer and network integrity." Computer Networks and ISDN Systems 17(2): 141-148.

Dowd, P. W. and J. T. McHenry (1998). "Network security: it's time to take it seriously." Computer 31(9): 24-28.

Deri, L. and S. Suin (2000). "Practical network security: experiences with ntop." Computer Networks 34(6): 873-880.

Fyodor (1998), Remote OS detection via TCP/IP stack ®ngerprinting, *[online:http://www.insecure.org/nmap/nmap-®ngerprinting-article.txt].*

Humberto T. Marques, N., C. D. R. Leonardo, et al. (2004). Characterizing broadband user behavior. Proceedings of the 2004 ACM workshop on Next-generation residential broadband challenges, ACM.

John, M., M. Ron, et al. (2008). Passive network forensics: behavioural classification of network hosts based on connection patterns, ACM. **42:** 99-111.

Kong, H.-s., M.-q. Zhang, et al. (2009). The Research of Simulation for Network Security Based on System Dynamics. Information Assurance and Security, 2009. IAS '09. Fifth International Conference on.

McNamara, R. (1998). "Networks — where does the real threat lie?" Information Security Technical Report 3(4): 65-74.

Michael Zink, K. S., Yu Gu, Jim Kurose (2009). "Characteristics of YouTube network traffic at a campus network – Measurements, models, and implications." Computer Networks 53(4): 501-514.

Muftic, S. (1988). "Security mechanisms for computer networks; current results of the CEC COST-11 ter project." Computer Networks and ISDN Systems 15(1): 67-71.

Pescatore, J. and G. Young. (2009, 12 October). "Defining the Next-Generation Firewall." Gartner RAS Core Research Note, from http://www.gartner.com.

Ruiliang, C., Z. Xin, et al. (2001). A distributed algorithm enhancing the connection quality and bandwidth utilization in wireless cellular networks. Computer Networks and Mobile Computing, 2001. Proceedings. 2001 International Conference on.

Tao, Z. and W. Chong (2008). Network Security Analysis Based on Security Status Space. Web-Age Information Management, 2008. WAIM '08. The Ninth International Conference on.

WAP Forum (June 1999), WAP White Paper, *[online:http://www.wapforum.com/what/whitepapers.htm]*.

(2010), "Palo Alto Network Next Generation Firewall Overview." from *[online:http://www.paloaltonetworks.com/literature/]*.