Universiti Teknologi MARA

Vulnerability Analysis on the Network Security by Using Nessus

Firkhan Ali b. Hamid Ali

MScIT

September 2004

Universiti Teknologi MARA

Vulnerability Analysis on the Network Security by Using Nessus

Firkhan Ali b. Hamid Ali

(Bachelor of Computer Science (Hons) UPM)

Independent study report is submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Information Technology
Faculty of Information Technology and Quantitative Sciences

September 2004

ACKNOWLEDGEMENTS

The great of praise is to Allah S.W.T for giving me the opportunity, time and effort to complete in this independent study report. Then, I really hope that it will contribute to the continuously knowledge in the future.

I want to express my deep appreciation to my supervisor, En. Abdul Hamid Othman that had gave me a good supervision, valuable of guidance and support to complete this study.

I am deeply indebted to En. Miswan Surip for his outstanding contribution that gives me permission to done this study at FTMM, KUiTTHO and including all the staffs of FTMM, KUiTTHO for their co-operation.

I am really appreciate the role that all lecturers of the Masters program especially A.P Dr. Isa Samat for their effort, dedication and support in sharing the knowledge and experiences in the field of IT.

I owe a great debt of gratitude to my mum, Rahmah Talib for her prays, advices and support along the way in my life. Thanks a lot to my father in law, Monhadi and mother in law, Kasini for supporting me along this study.

Lastly, I want to express my deep appreciation for the support, understanding and encouragement of my beloved wife, Norsalina Monhadi and two of our cute kids, Fatihah Insyirah and Muhammad Al-Fatih. Thanks a lot to all the contributors.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ATM	Asynchronous Transfer mode
CSU/DSU	Channel Service Unit/Data Service Unit
DoS	Denial of Service
HTML	Hypertext Markup Language
HVAC	Heating, Ventilation and Air Conditioning
IMAP	Internet Message Access Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standards
UDP	User Datagram Protocol
OSI	Open System Interconnection
NOC	Network Operating Center
NOS	Network Operating System
PDU	Protocol Data Unit
PBX	Public Branch Exchange
RFC	Request For Comments
RPC	Remote Procedure Call
SATAN	Security Administrator Tool for Analyzing Network
SNMP	Simple Network Management Protocol
PC	Personal Computer
UPS	Uninterruptible power Supply

ABSTRACT

Exploitation by attackers whose have breached the network security of some of the world's most venerable institutions and organization had become increased every year including in Faculty of Information Technology and Multimedia (FTMM), Kolej Universiti Teknology Tun Huessein Onn (KUiTTHO).

Within this type of attention, network security has gone from the as an extra services to the main services in a relatively short period in FTMM. The main purpose is to mitigate security risk and assure that their FTMM's digital assets are in safe and digital environment is become a better condition to the staffs and students.

Vulnerability analysis activities can help to identify the weaknesses and vulnerabilities in the computer network system at FTMM to prevent the attacks against it by the hackers or crackers. The idea is, done vulnerability analysis by using vulnerability scanning tools, Nessus to identify and fix these weaknesses or vulnerabilities before the attackers use them against the FTMM computer network system.

CHAPTER 1
PROJECT BACKGROUND

1.1 Introduction

Today, world have face very dangerous threats of cyber crime in the digital environment from a person to a big company like Yahoo, Amazon and etc. The most important is finding the way that it happens and how to protect and solve it.

On January 2004, Malaysian Computer Emergency Response Team or MyCERT had reported inside their web site about 157 websites in Malaysia had been hacking and exploit. This incident involved many organization websites including private sector and government.

This is the latest incident that happens in Malaysia in several months ago. According to the MyCERT, the last issue on this incident is happening because of two main reasons. Firstly is level of the network security awareness among webmasters or system administrators are very low. Secondly, the knowledge of the webmasters or system administrators is very low. They didn't make any security's assessment and evaluation to ensure the security on their network and systems are in the best condition.

Network Security analysis including vulnerability analysis is a chore that many system and network administrators tend to neglect. In today's IT climate of belt tightening, most of the system administrators have a mandate from the companies or organization to do

more with fewer resources. Proactive security measures are often low on management's list of priorities especially in Malaysia's organizations until some attacks had done and breach into one of the servers or network

According to the scenario and problem above, this project will make a study in vulnerability analysis on the network security by using open source's vulnerability scanning tools, Nessus at Faculty of Information Technology and Multimedia (FTMM), Kolej Univesiti Teknologi Tun Hussein Onn (KUiTTHO). This effort can be the best way and important things in addressing to this issue.

So, this report will provide an analysis of the vulnerabilities that make weaknesses on the computer network system in FTMM by using most popular open source tools, Nessus. The result of this analysis will provide including statistic of the types of vulnerabilities, possible attackers, possible information or data loss that will make weaknesses on the network and the suggestion of best steps or action should be taken to addressing the vulnerabilities that will find in the FTMM's network.

1.2 Significance of Study

FTMM will be able to use the result of this vulnerability analysis study on the network security to improve the network security in FTMM, KUiTTHO.

Doing this study in FTMM will enhance awareness to done network security assessment and ability of usage open source network security tools.

1.3 Aims

This paper is aim to highlight the critical issues on the security vulnerabilities that make weaknesses on the computer network system in FTMM, Kolej Universiti Teknologi Tun Hussein Onn (KUiTTHO).

1.4 Objectives

1. To scan the network security vulnerabilities and weaknesses by using open source tools, Nessus.

2. To analysis and identify overall of the network security's vulnerabilities that make weaknesses in the network including the general action should be taken on it.

1.5 Scopes of Work

As the time allocated for this study is more or less four months, it is essential to outline the scopes of works so that it will work as promised. This study of vulnerability analysis on the network security in FTMM will highlight with this three main things.

Firstly is done the vulnerability scanning on the network at FTMM by using open source tools. Secondly is overcome with the possible exploits and vulnerabilities in the computer network from the result of the scanning. Then, the analysis on the vulnerabilities from the

vulnerability scanning result will do. Lastly are the recommendations and suggestions to improve the network security according to analysis of the vulnerabilities.

Clearly, this study will be implemented to the selected host in range of IP addresses in certain of subnet computer network system in FTMM.

1.6 Project Approach & Methodology

This study will be conducted by the following tasks: -

Literature review for a study and gather much information about the: -

a) Network management concepts and methodology.
b) Network security concept and methodology.
c) Network security assessment concept, methodology and Open Source tools.

Vulnerability analysis on the network security at FTMM will be conduct by using vulnerability scanning open source tools, Nessus. The steps that will cover in this analysis are discovery, vulnerability scanning and vulnerability analysis.

1.61 Work Flow

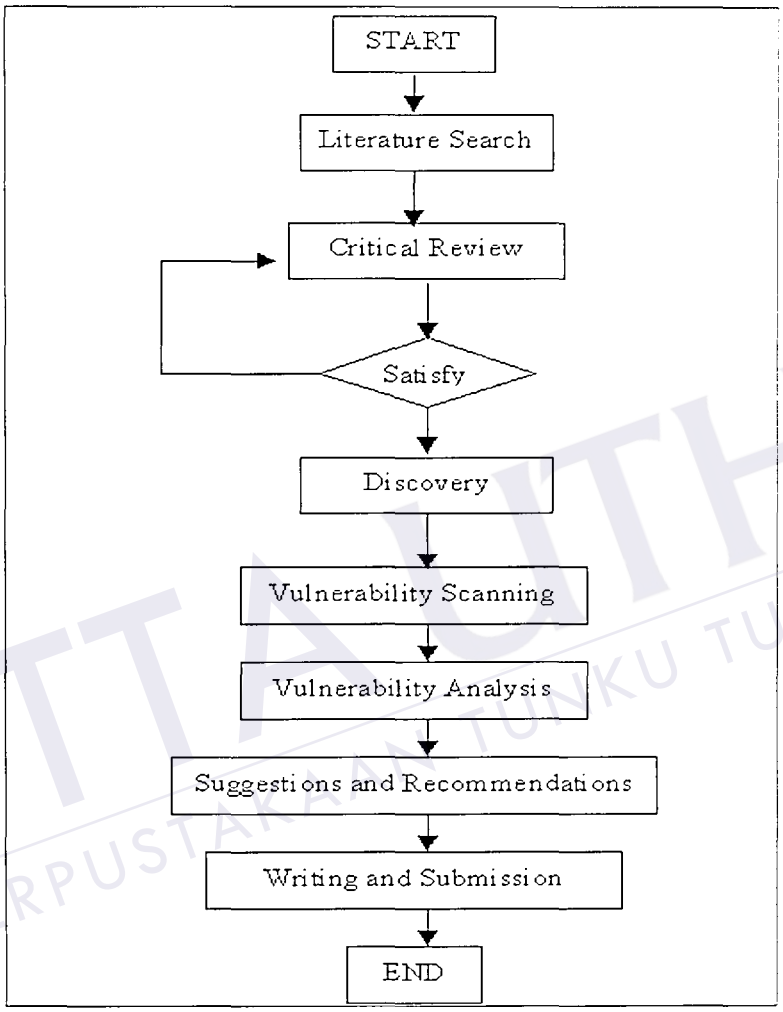

Figure 1.1: **Project's workflow**

1.7 Project Plan

Working Schedule

Table 1.1: **Working Schedule**

Year/Month	2004					
	May	June	July	August	Sept	Okt
Planning and Proposal	→					
Literature Search	→	→				
Critical Review		→	→			
Testing Network Security			→	→		
Analysis Data			→	→	→	
Recommendation and Suggestion			→	→	→	
Writing Dissertation		→		→	→	→

1.8 Limitation

The vast limitation in doing this project is in term of its time. So, to cope with time limitation, this study would only done vulnerability analysis for network security environment to the selected host in range of IP addresses in certain subnet computer network system in FTMM.

1.9 Summary

This is very though time for Malaysian organization including FTMM, KUiTTHO to face too many issues in the network security according to the news and statistic that had provided by MyCERT. All these things will be caused ICT facilities will be in damage and slow the process or usable use. This will be effect the quality and quantity of the productions for the organization and the business strategy for that organization is become fail.

This network security's problem is critical to many of the organization in Malaysia but analyzing it is a daunting if not impossible task. The solution is make security's assessment including this vulnerability analysis into the network system and the reporting according to the analysis must be consolidates the event data. Then, correlates that data into simplify, meaningful information that is easily understand by the many departments or staffs that need to access it.

The intent of this study is to provide useful tips and guidelines from the report of the vulnerability analysis to manage and minimize the vulnerabilities that make penetrations and possible attacks in the computer network system at FTMM, KUiTTHO. The risks or weaknesses from this report like a possible exploit, vulnerabilities or penetration are the potential of the computer network system attacks.

In addressing this risks of vulnerabilities, it's need to converge upon a core process for managing network security vulnerabilities by discovering all the network security aspects.

Then, do scanning these discovered assets over the network system for vulnerabilities. After that, do reporting and prioritizing these vulnerabilities that make the weaknesses on the network. Then, make the suggestions to solve on all these vulnerabilities that had found and its can become dangerous penetrations and attacks to the affected systems. Done the right actions according to the suggestions that we had make from the report to prevent the existing vulnerabilities in the network exploit by the attackers.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

Network management is more important things in the network computer system that will provide efficiency and effectiveness use of network. It has several functions including security part that will apply in any type of network topology

Network security is become first and very important criteria in any using of devices, system or to make any decision that regarding to the information system. There is because of more systems and computers are interconnected each other for easing to access by authorized users.

Then, to detect, protect and react from the threats and intruders, the network security assessment is important thing that need to be done in the organization. So, the testing and analysis in the network security by using network security tools can be done. It has three types of testing and analysis in the network security that includes: -

a. Penetration testing.
b. Vulnerability Assessment.
c. Audit.

There are many of open source vulnerability scanning tools that available on the Internet that can be use for vulnerability assessment on the network like Nessus, SARA, SATAN and others.

Then, to know whose are the attackers and what is methodology, steps and tools that they done on making an attack into the network is also important parts. This knowledge will map the ideas and steps to protect, detect react back if the network system in trouble by intrusions.

Lastly, ethical and policy in the network security is more important to the human that involved in network security because it will involve in integrity, availability and confidentiality of data, information and system.

2.2 Network Management

Main role in the network management concept is keeping up and running to maximum efficiency use of network while effectively managing is growth. There are five functional areas of Network management that consist of Fault/problem management, configuration management, accounting management, performance management and security management. It also known as FCAP that mean for Fault, Configuration, Accounting, Performance and Security. Then, these five functional areas will apply to 4 distinct, which are Local Area Network, Wide Area Network, Server/Network Operating System and Multi-area.

2.2.1 Functional Areas in Network Management

In the Network management concept to maintain keeping up and running to maximum efficiency while effectively managing is growth is very complex tasks. It has become the very though challenging in the network management processes. So, by dividing its tasks into five functional areas, the tasks of Network management processes can become easier to handle. As mention earlier before the components of this functional areas are consist as follows: -

a. Fault/problem management.
b. Configuration management
c. Accounting management
d. Performance management
e. Security management.

So, these of five functionalities are needed each other to perform the best computer network running especially in network security and network performance. The figure 2.1 will show the depending of all these 5 functionality in the network management as follows.

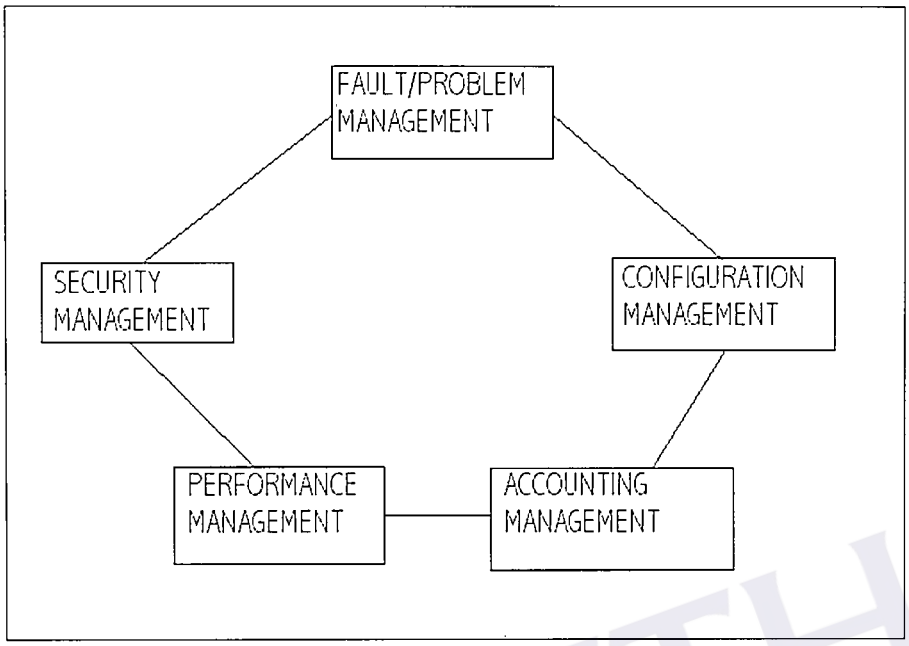

Figure 2.1: **Functional Areas of Network Management**

2.2.1.1 Fault/Problem Management

It defines network management's monitoring and messaging capabilities. The responsible of this functional are to identify problems proactively and effectively inform the systems staff.

Use of trouble ticketing system had enhanced the function of fault/correction management by tracking of fault events and will expand the logging. With this, it provides a repository of problem resolution information.

The effectiveness of this functional is fully depending on accurate trouble ticketing and asset tracking/management to reach the solution or accurate information.

The important elements in this functionality are Fault Detection, Fault Notification and Fault Correction.

These two of components, Fault Detection and Fault Notification are working together within reactive processes. Network Service Center will alert by alarm if nodes that are failure are observed and identified. Alarm will be displays in minutes to hours at fault management station.

Fault detection that had keep the past failure within the recommendation of system correction can be use to prevent and capture the future problems.

Lastly, Fault Correction is its element that has ability to remotely take remedial action on the occurrence problems by using the software called elements manager. It is the reactive processes. So, if the Network Service Center is on the power, it able to connect on the failure node or systems that occur over the existing network. So, the correction can be made in very fast before the customers aware about this problem.

2.2.1.2 Configuration Management

Configuration Management is one of the functional in the network management that has ability to control the changes in the operating status of a managed device and as same as

BIBLIOGRAPHY

'Awas! Pencerobohan laman web besar-besaran',
http://www.mycert.org.my/news/2004_01_28_01.html [30 May 2004]

Carne, E. (1999) Telecommunication Primer: Data, Voice and Video Communication (2nd edn), Prentice Hall PTR.

Davis, G.B. and Olson, M.H. (1985) Management Information System: Conceptual Foundations, Structure and Development (2nd edn), McGraw-Hill.

'Definition for Common Security Terms', http://www.mycert.org.my/securityterm.html [25 May 2004]

'Demonstrations' , http://www.nessus.org/demo/index.html [1 June 2004]

'Documentation' , http://www.nessus.org/decomentation.html [1 June 2004]

Dunsmore, B. and Skandier, T. (2002) Telecommunication Technologies Reference. Cisco Press.

'Ethical Hacking Techniques to Audit and Secure Web-Enabled Applications, Amit Klein, http://www.SanctumInc.com/pdf/Ethical_Hacking_Technique.pdf [30 May 2004]

Forester, T (1994) Computer Ethics, MT Press, Cambridge USA.

Hatch, B., Lee, J. and Kurtz G. (2001) Hacking Linux Exposed: Linux Security and Solutions, Osborne/McGraw-Hill.

'How Home Networking Works',
http://computer.howstuffworks.com/home-network.htm [1 June 2004]

'Introduction' , http://www.nessus.org/intro.html [1 June 2004]

Kane, J., Lindholm, C. (2001) Cisco Networking Academy Program: First Year Companion Guide (2nd Edition),Cisco Press.

Norton, P and Stockman, M. (1999) Peter Norton's Network Security Fundamentals. SAMS Publishing.

Northcutt, S., Zeltser, L., Winters, S., Frederick, K.K. and Ritchey, R.W. (2003) Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers and Intrusion Detection Systems, New Riders.

O'Brien, J.A. (1998) Managing Information Systems (4th Edition), Mc Graw-Hill.

'Plugins' , http://www.nessus.org//plugins/plugins.html [1 June 2004]

Reynolds,G (2003) Ethics in Information Technology. Boston: Thompson Course Technology

Scambray, J., Mcclure, S. and Kurtz G. (2001) Hacking Exposed: Network Security and Solutions, Osborne/McGraw-Hill.

'Security FAQs', http://www.mycert.org.my/faq.html [20 May 2004]

Stallings, W. (2000) Network Security Essentials: Application and Standards, Prentice Hall.

Tipton, H.F. and Krause, M. (2000) Information Security Management Handbook (4th Edition), Auerbach Publications.

'Top 20 Exploits', http://www.sans.org/top20/index.php [20 May 2004]

Williams, B.K., Sawyer and Hutchinson, SE (1995), Using Information Technology, Richard D. Irwin, Inc.

Zacker, C. (2001) Networking: The Complete Reference, Osborne/McGraw-Hill.