Universiti Teknologi MARA

Network and Application Security Assessment

Norizam Idris

Independent Study submitted in partial fulfillment of the requirement
for the degree of

Master of Science

**Faculty of Information Technology and
Quantitative Science**

September 2004

ACKNOWLEDGEMENT

Al Hamdullilah.

First of all, I would like to thank and appreciation to my supervisor, En Abdul Hamid othman from the Faculty of Information technology and Qualitative sciencefor all his help and advise during all of the work toward this independence study.

Secondly, I wish to thank my colleagues for helping and sharing the information regarding to this project.

I would also Thank Mr. Kamaruddin Tahir, Deputy Director (HRMIS) for allowing me to study and investigate network and applications in Data center.

Finally , my parent and friends are always my firmest support through all my life.

Thank you

ABSTRACT

Assessment of network and application security is the process of detecting, recording and auditing to come out with a schema network security measurement.

Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

This section provides a basic introduction to the technologies that underlie the network technology. It was written with the novice end-user in mind and is not intended to be a comprehensive survey of all network -based technologies

The security assessment that was conducted focus on four distinct areas that were assessed separately. These areas were Application security, Host security, Network Security and Disaster Recovery

The aims of the Applications Security Assessment was to identify and analyze security flaws found in HMRIS Data Center as well as recommend solution to eliminate or minimize the risk. The Host security Assessment on the other hand was aimed at identifying, analyzing and proposing corrections for security vulnerabilities of identified critical server hosting the HRMIS system.

In the environment where the HRMIS system is situated, the Internet is the main point of entry for any possible threats. The Network security Assessment aimed at recommending best practice mechanisms and control in order to eliminate possible attacks from this environment. Finally, the aims of Disaster Recovery Assessment were to determine the state of readiness of HRMIS system Recovery major disaster occurs.

From the Application Security Assessment, it was found that HRMIS application is high vulnerable to attacks by users from both the internal and external networks. It is recommended that action be taken immediately in order to rectify

this problem as user interaction is primarily with the online application. After performing the Host security Assessment we can determine whether the host operating system have been securely configured. Default installations are highly vulnerable as unnecessary and often-insecure service is left running and the latest security patches and updates are not installed.

Result from network security Assessment that will found weather it is imperative to install Intrusion Detection System to monitor the network as well as log server for the safe keeping of logs, while incident handling

In conclusion, the current state of the HRMIS environment demands complete security controls and mechanism in order to be safeguarded in every aspect in accordance to best practice adopted worldwide. In view of this,

It also recommended that the current security practice be enhanced and ideally be implemented in Phase 2 of the HRMSI project. By adding more relevant security control and mechanisms such as secure web servers, secure Socket layer (SSL) connections and the usage of digital signature on smart cards (Mykad) for authentication will not only to ensure the confidentiality and integrity of the information, but also to maintain the reliability of the HRMIS environment itself.

TABLE OF CONTENTS