THESIS

THE USE OF INTRUSION PREVENTION SYSTEM TO INCREASE COMPUTER SECURITY

NAJIB BIN LIMUN

UNIVERSITI TEKNOLOGI MARA

NOVEMBER 2005

THESIS

THE USE OF INTRUSION PREVENTION SYSTEM TO INCREASE COMPUTER SECURITY

by

NAJIB BIN LIMUN
2003323420
CS225

In partial fulfillment of the requirement for the
BACHELOR OF SCIENCE (HONS) IN DATA COMMUNICATION AND NETWORKING

A project paper submitted to

FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCE
UNIVERSITI TEKNOLOGI MARA

Approved by the Examining Committee:

Encik Adzhar Abdul Kadir Project Supervisor

En Ahmad Yusri Dak Examiner

NOVEMBER 2005

DECLARATION

I hereby declare that the work in this report is my own except for quotations and summaries which have been acknowledge.

24th JANUARY 2006 NAJIB BIN LIMUN

2003323420

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and Most Merciful. All praise be to Allah, for all the bless that he gave, finally I can complete my project upon the date end.

First and foremost, I would like to express my deepest appreciation and thanks to my dedicated supervisor, Mr. Adzhar Abdul Kadir, for his guidance, ideas, supporting and advice in completing the project. I am very lucky to have him as a supervisor as he is an experience lecturer.

Special thanks to other lecturers and staffs who have also help me in completing my project. Not forgotten, my friends who have willingly to share their knowledge with me. I feel very fortunate to have the advice and guidance of many talented people who have many experience and knowledge in all aspect of network, open source and security tools. They shared their ideas with me.

Lastly, I would like to express my gratitude to my beloved parent who have supporting me. These are the people who have always giving me a moral support in completing my project. Thank you for all the person who have help me. May Allah bless you.

ABSTRACT

Network intrusion prevention systems provide an important proactive defense capability against security threats by detecting and blocking network attacks. This task can be highly complex and traditional firewall system are currently not capable of handling fast attack through the operating system. The problems arise when many exploits attempt to take advantage of weaknesses in every protocols that are allowed through our perimeter firewalls, and once the Web server has been compromised, this can often be used as a springboard to launch additional attacks on other internal services. Once a "rootkit" or "back door" has been installed on a computer, the hacker has ensured that he will have unfettered access to that machine at any point in the future. Thus, iptables also called as Netfilter can also be implement as an intrusion prevention system. Iptables works by filtering the traffic flow between your computer and the Internet. It can limit access to and from the Internet to only specific computers on your network. It can also limit the type of communication, selectively permitting or denying various Internet services. Hence, to harden the iptables rule, another tool need to be apply to work with the iptables rule script. The psad tool is good in implementing some additional feature like an e-mail alert and logfile analysis.