COVERT CHANNEL: NETWORK STEGANOGRAPHY DEPLOYMENT

By

NURUL MAJDI BINTI MD ALI

(2004633671)

Supervised by

PROF. MADYA DR. SAADIAH YAHYA

A project research paper submitted to

FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCES

UNIVERSITI TEKNOLOGI MARA

In partial fulfillment of requirement for the

BACHELOR OF SCIENCE (Hons.) IN DATA COMMUNICATION AND NETWORKING

UNIVERSITI TEKNOLOGI MARA

SHAH ALAM, SELANGOR

NOV 2005

ACKNOWLEDGMENT

All praises to Allah s.w.t for all His bless that help me on completing this research project. On this opportunity, I would like to show gratitude for those who had involved in contributing the idea and support either directly or indirectly along making this research project until it is complete. Special thanks to my supervisor, Dr Saadiah Yahya for her encouragement, guidance, comment and ideas that led me in producing a better quality research project. To En Adzhar who give me a great guidance, encouragement and tolerance. Your clarification is very pleasure.

Last but not least, to all Computer Technology and Networking lecturers and my colleagues and other in the faculty, who are simply too numerous to indicate, thanks to all encouragement and support given. To my parents and closest friends, it is all thank you so much that I could say. All the assist and support is much appreciated. Finally to all mentioned here, may Allah will reciprocate all of them for all those support. Thank you for everything.

To all the aforementioned, may Allah bless all of you.

Nurul Majdi binti Md Ali.
2004633671
BSc. Data Communication and Networking

ABSTRACT

Steganography is one of the major techniques used to hide the existence of communication that lies between two overt parties. Steganography also denoted by art of hiding communication. This work relates the areas of steganography, network protocols and security for practical data hiding in communication networks employing TCP/IP. This project major focus is to deploy steganography on network protocol using *covert_TCP* tool. This tool uses 3 methods in order to employ steganography at TCP/IP header; IP identification encoding, TCP sequence number encoding and ACK "bouncing" server method. We also employ network steganography in two different network environment which is on transmission on single host (loopback interface) and inter local area network. After that phase, we analyze packet income and out the network. We used network sniffer tool, tcpdump to dump all the packet and analyze the accuracy of the data transmit using covert channel as employ by *covert_TCP*.

TABLE OF CONTENTS