UNIVERSITI TEKNOLOGI MARA

EVALUATION EFFECTIVNESS HYBRID IDS USING SNORT WITH NAIVE BAYES TO DETECT ATTACKS

SAFWAN MAWLOOD HUSSEIN

Dissertation submitted in partial fulfilment of the requirement of the

requirements for the degree

Master of Science in Computer Networking

Faculty of Computer and Mathematical Sciences

January 2012

ABSTRACT

The vast amount of attacks over the Internet makes the computer users and many organizations under potential violation of security. IDS monitor the network to observe suspicious actions going on in a computer or network devices.IDS with using one approach has ability only to detect either misuse or anomaly attacks. This research proposed hybrid IDS by integrated Snort with Naive Bayes to enhance system security to detect attacks. This research used KDD Cup 1999 dataset for test provided hybrid IDS. Accuracy, detection rate, time to build model and false alarm rate used as parameter to measure performance between hybrid Snort with Naive bayes, Snort with J48graft and Snort with Bayes Net. The result shows that there are slight differences between all the three paradigms.

ACKNOWLEDGEMENT

In the name of Allah, the most gracious, most merciful and Him a line is worthy of all praise.First and foremost, my sincere gratitude goes to my supervisor Dr. Fakariah Hani Mohd AH. For encouragement, guidance, critics, without her help this dissertation would never had been done. I am especially grateful to Mr. Hameed Othman , whose provide me equipments and help me to solve many problems in technical part.

I also wish to acknowledge all my colleagues at UiTM University, especially Badri Ali,Mohd Hidzwan ,Asnita Hashim ,Mohammed Sadqi, for their insightful discussions on research. In addition I would like to thank all my dearest friends for their encouragement during this dissertation. Finally I would like to take this opportunity to express my deepest, acknowledgement to my parents, brothers and sisters, for their love and encouragement throughout the work .1 offer my best regards and blessings to all of you.

TABLES OF CONTENTS