UNIVERSITI TEKNOLOGI MARA

NETWORK INTRUSION DETECTION IN INTERNET SERVICE PROVIDER (ISP)

AINI BINTI AHMAD

Dissertation submitted in partial fulfillment of the requirements
for the degree of
Master of Science in Telecommunication and Information Engineering

Faculty of Electrical Engineering

July 2017

ABSTRACT

DDoS – is a volumetric attack that comes from multiple sources toward a targeted object (website and servers) which its intention either to make the targeted object unavailable for legitimate user. It would bring massive impact to the end user where can bear down the network, the website/server cannot be reach especially when the targeted object is related to organization that provide services like banking, education , insurance , transportation under attacks. They been overwhelming resources with huge data or queries.

This paper presented a study and performance of intrusion detection system that currently being implemented in the ISP's network. This paper covers one part of the ISP areas known as IP core department. A network tool known as Anti-DDoS Protection by Arbor has been used in the analysis. From the results obtained, it is found that UDP Flood and DNS Flood contribute most attacks towards particular target in the ISP.

ACKNOWLEDGEMENT

In the Name of Allah, the Beneficent, the Merciful

First praise is to Allah S.W.T, the Almighty, on whom ultimately we depend for sustenance, guidance and for His willing and blessing in giving me the opportunity and strength to complete my Master's degree generally and my final year project specifically. Second, my sincerely appreciation goes to my supervisor Assoc. Prof. Ruhani Bt. Ab Rahman, whose guidance, careful reading and constructive comments was very valuable. Her timely and efficient contribution helped me shape this thesis into final form and I express my sincerest appreciation for her assistant in any way that I may have asked throughout the process of completing this thesis.

I also wish to thank the programme of Master Science in Telecommunication and Information Engineering, its leadership and the staff for providing me with an academic base, which has enable me to take up this study. I would like to express my gratitude to all lecturers in my graduate career Dr. Nur Emileen Abd Rashid, Dr. Azita Laily Binti Yusof, Assoc. Prof. Dr Habibah Hashim, Assoc. Prof. Dr. Norsuzila Ya'acob, Dr. Azlina Binti Idris, Assoc. Prof. Dr. Mohd Tarmizi Ali, Dr. Zuhani Khan and Dr. Darmawaty Mohd Ali for everything they have taught me about telecommunication that shaped me into what I am today and made my thesis possible. Special thanks to all those their names do not appear here who have contributed to the successful completion of this study.

Next, I would like to thank my friends;

classmates, my senior and all EE700 students who help me and gave me suggestions. I

TABLE OF CONTENTS