ANALYZING INSIDER THREATS BASED ON DNS NETWORK TRAFFIC

(CASE STUDY IN ORGANIZATION XYZ)

By

Kris Ivan Santosa

12112012

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
EduTown BSDCity
Tangerang 15339
Indonesia

August 2016

ANALYZING INSIDER THREATS BASED ON DNS NETWORK TRAFFIC

(CASE STUDY IN ORGANIZATION XYZ)

By

Kris Ivan Santosa

12112012

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
EduTown BSDCity
Tangerang 15339
Indonesia

August 2016

Revision after the Thesis Defense on 21 July 2016

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in this thesis.

Kris Ivan Santosa

Student Date

Approved by:

Charles Lim, M.Sc., ECSA, ECSP, ECIH, CEH, CEI

Thesis Advisor Date

Alva Erwin, ST, M.Sc., MTI

Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc

Dean Date

ABSTRACT

ANALYZING INSIDER THREATS BASED ON DNS NETWORK TRAFFIC
(CASE STUDY IN ORGANIZATION XYZ)

By
Kris Ivan Santosa
Charles Lim, M.Sc., ECSA, ECSP, ECIH, CEH, CEI, Advisor
Alva Erwin, ST, M.Sc., MTI, Co-Advisor

SWISS GERMAN UNIVERSITY

The Internet is a media for people to communicate with each other. The Internet also full of threats for it's users. This makes security one of the problem of the Internet. This is also one of the problem for organizations that use the Internet.

Organization have two types, external threats and insider threats. External threats are threats that came from outside of the system and insider threats are threats that came from inside of the system. Most of organizations prioritize external threats over insider threats. Although insider threats are the dominant in security breaches and the number of insider breaches are increasing.

DNS is one of the main function of Internet. One of DNS function is to resolve domain name to IP address. Most of the user use DNS to be able to connect to the Internet including malicious hackers. DNS can also be used to detect insider threat using the features of insider threats which can detect unknown insider threats. This research aims to detect insider threats using DNS based detection.

The features of the insider threats will be extracted from the raw DNS queries. These features will be preprocessed to remove the unused data and will be clustered. From the clusters, it can show the features of insider threats.

This research is able to suspect the clusters. The result is that there may exist insider threats in organizations and the most frequent suspects of insider threats are botnet which categorized as misuse in insider threat classification. There also some clusters that benign but abnormal traffic that still have few features of insider threats. The recommendation for the insider threats mitigation in organizations are using features of botnets to filter the DNS packets and block the domain once it reach certain threshold.

Keywords: clustering, insider threat, DNS, machine learning, data mining

DEDICATION

I dedicate this work to my parents that always supporting me and give their best to take care of me.

ACKNOWLEDGEMENTS

The author would like to express deepest gratitude to Mr. Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI and Mr. Alva Erwin, ST, M.Sc., MTI for their guidance during the completion of this research. With their support, this research can reach this point.

The author is also grateful for guidance and support from his friends, seniors during this research development. Thanks to the numerous support of his friends and seniors that the author could complete this research. Especially Mario Marcello M.Kom for his guidance through out the research.

The author also would like to thank the author's family for their moral supports. It is because of their support and prayer that the author able to complete this research.

Contents