DETECTING NEW NETWORK SECURITY THREATS USING DNS AND NETFLOW TRAFFIC

By

Rinkel Hananto
11302014

BACHELOR'S DEGREE
in

Information Technology
Faculty of Engineering and Information Technology

SGU®
SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat no. 15, Alam Sutera
Kota Tangerang, Banten 15143
Indonesia

August 2017

Revision after the Thesis Defense on 19 July 2017

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 the thesis.

SGU ® SWISS GERMAN UNIVERSITY

Rinkel Hananto

Student Date

Approved by:

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

Thesis Advisor Date

Ir. Heru Purnomo Ipung, M.Eng

Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc

Dean Date

ABSTRACT

DETECTING NEW NETWORK SECURITY THREATS
USING DNS AND NETFLOW TRAFFIC

By

Rinkel Hananto
Charles Lim, M.Sc., ECSA, ECSP, ECIH, CEH, CEI, Advisor
Ir. Heru Purnomo Ipung, M.Eng, Co-Advisor

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY

Uncontrolled network traffic in organizations could lead to many malicious threats, such as data breach, server compromised, server availability, and others. Many network security threats can be detected by monitoring and analyzing network traffic. One of the emerging threats is Domain Name System (DNS) Distributed Denial of Service (DDoS) attack, which flood the authoritative DNS server with large amount of DNS request. Monitoring and understanding the traffic data could prevent such attack. Therefore, we present a technique for detecting DDoS attack by correlating DNS and NetFlow traffic. The idea is to show that NetFlow can be used as the first DDoS indicator and then DNS is used to evaluate and verify the DDoS. We propose to model the ratio DNS NXDOMAIN response and Information Entropy feature using statistical approach. The traffic is under anomaly condition if the traffic is outside from the standard deviation threshold. We discovered low volume and high volume DDoS attack using statistical approach during the experiment. Attackers' botnet utilizes DNS to do DDoS called DNS water torture attack or random subdomain attack. The results of the experiment can be used to prevent the attack such as domain blacklist.

Keywords: Botnet, DNS, DDoS, Information Entropy, NetFlow, Network Anomaly Detection, Network Security Threats, Traffic Correlation

© Copyright 2017
by Rinkel Hananto
All rights reserved

DEDICATION

I dedicate this to my mother, my father and nine TWICE members; Minatozaki Sana, Hirai Momo, Im Nayeon, Kim Dahyun, Myoui Mina, Park Jihyo, Son Chaeyoung, Chou Tzuyu and Yoo Jeongyeon, who makes life worth living.

SWISS GERMAN UNIVERSITY

ACKNOWLEDGEMENTS

I would like to deliver my sincere gratitude to my advisor, Mr. Charles Lim, my co advisor Mr. Heru Ipung Purnomo, and Dr. Lukas for the limitless support and time during my thesis research, for their patience, motivation, and immense knowledge. Their knowledge and guidance help me in all the time of research and writing of this thesis and related researches.

I would like to thank PT Cyberindo Aditama (CBN) for allowing me the opportunity to conduct my research and work as an intern in the company. I specifically present my gratitude to Rommy Kuntoro, Achmad Yahya Sjarifuddin, Royke Kaligis, and Anderson Lumbantobing for guiding and helping me during the internship and research period at CBN. I would also like to thank the team in Network Operations Center department for cooperating and aiding me with the knowledge and resources needed during the period.

I would also like to thank you to Hansen Chitrahadi and Jason Yapri for mentioning my name in his thesis acknowledgements.

SWISS GERMAN UNIVERSITY

TABLE OF CONTENTS

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY