NETWORK FORENSIC USING PACKET ANALYSIS
AT PERIMETER SEGMENT TO DETECT AND PREDICT
DNS AND HTTP BASE SECURITY ATTACK OR INTRUSION

By

WIDODO LAKSONO PUTRO
22051002

MASTER'S DEGREE
in

MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY

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

June 2021

NETWORK FORENSIC USING PACKET ANALYSIS AT PERIMETER SEGMENT TO DETECT AND PREDICT DNS AND HTTP BASE SECURITY ATTACK OR INTRUSION

By

WIDODO LAKSONO PUTRO
22051002

MASTER'S DEGREE
in

MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY

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

Revision after Thesis Defense on 15 July 2021

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

WIDODO LAKSONO PUTRO

Student

Date

Approved by:

DR. Charles Lim, B.Sc, M.Sc.

Thesis Advisor

Date

Kalpin E Silaen, S.Si, M.Kom

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium, S.Kom., M.Sc

Dean

Date

ABSTRACT

Network Forensic Using Packet Analysis at Perimeter Segment
to Detect and Predict DNS and HTTP Base Security Attack or Intrusion

By

Widodo Laksono Putro

DR. Charles Lim, B.Sc, M.Sc
Advisor
Kalpin E Silaen, S.Si, M.Kom
Co-Advisor

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY

Today the cyber threat, attack and intrusion growing in term of quantity and complexity along the fast growing of internet services utilization where people in any enterprise establish connection, communication and transaction with digital public resources. These resources mostly available via web access where HTTP(S) and DNS protocol been used. The attacker then use HTTP(S) and DNS protocol evasion to make the action undetected by the traditional security system such as perimeter Firewall, IDS or even legacy antivirus at endpoint side. This research covers the approach to resolve this issue by utilizing network forensic method to detect and predict HTTP(S) and DNS base security attack or intrusion.

This Thesis expands the existing generic network forensic at certain steps mainly in analysis step. The process includes copying the real network traffic by doing packet capture technique in perimeter network area and observe DNS and HTTP(S) traffic. The data which is in the form of pcap file then be extracted to have suspicious indicative features of the protocols to detect malicious indicator and then map to MITTRE ATT&CK framework to get the attack steps have been already executed.

The detection also utilizes two-layer filtering which based on the blacklisting filtering and features base filtering. Some features of malicious HTTP(S) and DNS protocol includes randomized DNS queries, suspicious user-agent, URI and Host value.

The result of detection then will become reference for existing traditional security system enhancement.

In this research with the network forensic approach also has advantage in detecting the malicious indicators related with DNS and HTTP(S) protocols -which the protocols commonly allowed by legacy security system such as common perimeter firewall. The suspicious features in the connection and the indicative infected computer can be investigated.

Keywords: Network Forensic, packet capture, detection

SWISS GERMAN UNIVERSITY

© Copyright 2021
by WIDODO LAKSONO PUTRO
All rights reserved

DEDICATION

I dedicate this thesis work to my beloved family, my wife Rahayu Kusumaningsih who always giving support to my continues study and future achievement. Also, to my son Evan Haryo Widodo who always become motivation and spirit to embrace the future.

SWISS GERMAN UNIVERSITY

ACKNOWLEDGEMENTS

I would like to express My gratitude to DR. Charles Lim, B.Sc, M.Sc, and Kalpin E Silaen, S.Si, M.Kom, as my thesis advisors for the dedication to giving intensive guidance, advise and motivation throughout this thesis.

I would also like to thank to friends during the study who motivate and learn each other making me always motivated and focus to finish this work.

Lastly thanks also to SGU staff which support any of supporting thing which make this thesis work is completed

SGU ®
SWISS GERMAN UNIVERSITY

TABLE OF CONTENT

ABSTRACT 4
DEDICATION..... 7
ACKNOWLEDGEMENTS..... 8
TABLE OF CONTENT..... 9
LIST OF FIGURES 11
LIST OF TABLES..... 12
CHAPTER 1 - INTRODUCTION 14
1.1 Background 14
1.2 Research Problem..... 15
1.3 Research Objective..... 16
1.4 Research Question..... 16
1.5 Scope of Study 16
1.6 Significance of the Study 17
1.7 Hypothesis..... 17
1.8 Thesis Structure..... 17
CHAPTER 2 - LITERATURE REVIEW 19
2.1 Enterprise Internet Technology and Issue..... 19
2.2 Traditional Threat Detection 21
2.3 Network Forensic (Framework and Beneficial)..... 22
2.4 Benign HTTP(S) and DNS Protocol Behaviour 26
2.5 General Malicious Traffic Behaviour 34
2.6 HTTP(S) and DNS Base Malicious Traffic Behaviour..... 35
2.7 Malicious Traffic Detection Base on Machine Learning Algorithm Approach..... 37
2.8 Evidence Finding Using Host (Computer) Base Forensic Approach 40
2.9 MITTRE ATT&CK..... 41
2. Related Work..... 42
CHAPTER 3 – RESEARCH METHODS..... 47
3.1 General Research Methodology..... 47
3.2 Research Framework..... 47
3.3 Data Sourcing Method 50
3.3 Data Analysis and Evaluation 51

SWISS GERMAN UNIVERSITY

3.3.1 DNS Traffic Filtering 51
3.3.2 HTTP(S) Traffic Classification 52
3.4 Validation 55
3.4.1. Validation by Host (Computer) Base Forensic 55
3.4.2 Validation by MITRE ATT&CK Framework 56
CHAPTER 4 – RESULTS AND DISCUSSIONS 57
4.1 System Experiment Overview 57
4.1.1 Experiment Setup (architecture) 57
4.1.2 Data Collection 58
4.2 Analysis and Evaluation 64
4.3 Validation 74
CHAPTER 5 – CONCLUSIONS AND RECOMENDATIONS 84
5.1 Conclusions 84
5.2 Recommendation 85
5.3 Future Work 86
GLOSSARY 87
REFERENCES 89
APPENDIX 94
CURRICULUM VITAE 97

SWISS GERMAN UNIVERSITY

LIST OF FIGURES

Figure 1-1 Common Protocol To Be Attack (Kumar, 2016)...................................... 14
Figure 2-1 Global Internet Penetration (Hootsuite & We Are Social (2019), 2021) . 19
Figure 2-2 Threat Report by SonicWall(SonicWall, 2021).. 20
Figure 2-3 Statistic of malware connection using TLS (HTTPS)(cisco, 2018) 21
Figure 2-4 HTTP Protocol Flow.. 26
Figure 2-5 DNS Hierarchy 27
Figure 2-6 DNS Request Response Messaging 28
Figure 2-7 TCP to HTTP Connection.. 29
Figure 2-8 Messaging in HTTP 30
Figure 2-9 HTTP - HTTPS differences 31
Figure 2-10 HTTPS Session Establishment Process 32
Figure 2-11 Element in the X509 Public Key Certificate Format 33
Figure 2-12 MITTRE ATT&CK Matrix(The MITRE Corporation, 2015)................. 42
Figure 3-1 General Research Method.. 47
Figure 3-2 Generic Network Forensic Framework... 48
Figure 3-3 Expanded Network Forensic Framework 49
Figure 3-4 Two Layer Detection Framework.. 49
Figure 3-5 Computer Forensic Steps 56
Figure 3-6 MITTRE ATT&CK Workflow... 56
Figure 4-1 Experiment Set Up.. 57
Figure 4-2 pcap file with higher size 59
Figure 4-3 pcap for Case-1 (6 April 2021) 59
Figure 4-4 pcap for case 2 (6 april 2021) 60
Figure 4-5 pcap of case-3 (25 May 2021) 61
Figure 4-6 pcap for case-4 (15 – 16 June 2021) 62
Figure 4-7 pcap for Case-5 (14 april, 26 april and 16 June 2021).............................. 63
Figure 4-8 pcap for case-6 (18 June 2021) 64
Figure 4-9 IP quality score case-1 65
Figure 4-10 IP Reputation Check case-2 66
Figure 4-11 URI value for Case-2 66
Figure 4-12 Hybrid Analysis Output for click.netsuite.com 67

SGU ® SWISS GERMAN UNIVERSITY

Figure 4-13 IP quality score for Case-3 67
Figure 4-14 IP quality score for case-4 68
Figure 4-15 user_agent observation 68
Figure 4-16 Common user_agent Parameter (whatismybrowser.com, 2021) 69
Figure 4-17 DNS query classification for suspicious indication 69
Figure 4-18 IP quality score for case-6 70
Figure 4-19 Host Value 71
Figure 4-20 svchost.exe process list 74
Figure 4-21 svchost checker 75
Figure 4-22 svchost.exe list in filesystem 75
Figure 4-23 svchost.exe malware indicators using PEStudio 76
Figure 4-24 string list 76
Figure 4-25 Certificate (expired) 77
Figure 4-26 imported dll. by suspicious svchost.exe file 77
Figure 4-27 Process List 78
Figure 4-28 dns.exe directories 78
Figure 4-29 malicious indicator in first dns.exe file save in c:\windows\system32\... 79
Figure 4-30 string list 79
Figure 4-31 another dns.exe file malicious indicator 80
Figure 4-32 MITTRE ATT&CK mapping 80
Figure 4-33 malicious detection by Hybrid analysis 81
Figure 4-34 MITTRE ATT&CK Mapping 82
Figure 4-35 Security Software Discovery Technique 82

LIST OF TABLES

Table 2-1 Computer and Network Forensic(Joshi and Pilli, 2016) 24
Table 2-2 Network Security and Forensic(Joshi and Pilli, 2016) 24
Table 2-3 Packet Capture and Log Collection 25
Table 2-4 HTTP Request Method 30
Table 2-5 HTTP Header Parameter 31

SWISS GERMAN UNIVERSITY

Table 2-6 C&C Characteristic(Acarali et al., 2016) 35
Table 2-7 Features for DGA Detection by Ren(Ren et al., 2020) 38
Table 2-8 Features for DGA Detection by Hwang... 38
Table 2-9 Features for DGA Detection by Tang(Tang et al., 2020) 38
Table 2-10 HTTP Periodicity Features... 39
Table 2-11 HTTPS Multi Categories Features 39
Table 2-12 Process List (from memory capture) with connection information 40
Table 2-13 Related Work Evaluation 43
Table 3-1 Defined DNS Features 52
Table 3-2 HTTP Feature base on periodicity 52
Table 3-3 HTTP Request Header Features... 53
Table 3-4 HTTPS Features 54
Table 4-1 Data Collection Summary 58
Table 4-2 Analysis and Evaluation Summary 71
Table 4-3 malicious indicators 82

SWISS GERMAN UNIVERSITY