HONEYPOT FINGERPRINT IDENTIFICATION TO ENHANCE ITS DECEPTION TO ATTACKERS

By
Rasyid Naif Dahbul
12112017

BACHELOR’S DEGREE
in

INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
EduTown BSDCity
Tangerang 15339
Indonesia

August 2016

HONEYPOT FINGERPRINT IDENTIFICATION TO ENHANCE ITS DECEPTION TO ATTACKERS

By
Rasyid Naif Dahbul
12112017

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 acknowledgment is made in this thesis.

SGU ®
SWISS GERMAN UNIVERSITY

Rasyid Naif Dahbul

Student — Date

Approved by:

Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI

Thesis Advisor — Date

James Purnama, M.Kom, M.Sc.

Thesis Co-Advisor — Date

Dr. Ir. Gembong Baskoro, M.Sc

Dean — Date

ABSTRACT

HONEYPOT FINGERPRINT IDENTIFICATION TO ENHANCE ITS DECEPTION TO ATTACKERS

By
Rasyid Naif Dahbul
Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI, Advisor
James Purnama, M.Kom, M.Sc., Co-Advisor

SWISS GERMAN UNIVERSITY

Honeypots are a great way to learn about unknown and new network-related attacks, it creates a decoy and record all activities that are happening on that system. Because honeypots are now popular and more deployed by network administrators, malicious attackers will try to find honeypot's weaknesses by searching its fingerprints. This research looks at the weakness of honeypots, which is fingerprints. The threat modeling methodology that are used helps the research by understanding the security model of the honeypot. Using threat modeling methodology, we are able to enhance the honeypots deception by configuring the honeypots itself. Review from security experts further validate the enhancements of the honeypots by providing instructive feedback for this research.

SWISS GERMAN UNIVERSITY

Keywords: Honeypot, Security, Fingerprint, Deception, Detection, Network

SWISS GERMAN UNIVERSITY

© Copyright 2016
By Rasyid Naif Dahbul
All rights reserved

DEDICATION

I dedicate this thesis to my parents, whom always love me and took care of me unconditionally. I also dedicate this thesis to my brothers and sister, who have provided the help I need.

SWISS GERMAN UNIVERSITY

ACKNOWLEDGEMENTS

I would like to express my most profound appreciation to Mr. Charles Lim and Mr.James Purnama for the time, support, counsel, and direction given all through this research and the culmination of this thesis report. It is a direct result of their inestimable commitments that this research report and the entire task can be completed. Without them, this research may not be finished at all. And I would like to thank the experts, Mr. Lucas and Mr. Tan Kean Siong for their expert review and suggestions, it helped this research exceptionally.

I would like to thank all of my friends for their helpful advices and for being there when I needed them. This journey may not be the same without them.

But, the most important people are my family. I thank my whole family for their unconditional support. It is because of them that I become a better person.

SWISS GERMAN UNIVERSITY

Contents

STATEMENT BY THE AUTHOR 2

ABSTRACT 3

DEDICATION 5

ACKNOWLEDGEMENTS 6

TABLE OF CONTENTS 10

LIST OF FIGURES 11

LIST OF TABLES 12

1 INTRODUCTION 13
1.1 Research Background . . . 13
1.2 Research Problem . . . 15
1.3 Research Objectives . . . 15
1.4 Research Questions . . . 15
1.5 Significance of Study . . . 15
1.6 Research Scope . . . 16
1.7 Research Limitation . . . 16
1.8 Hypothesis . . . 16
1.9 Document Structure . . . 16

2 LITERATURE REVIEW 18
2.1 Internet Security . . . 18
2.2 Cyber Deception . . . 19
2.3 Honeypots . . . 20
2.3.1 High-interaction Honeypots . . . 22
2.3.2 Low-interaction Honeypots . . . 22
2.3.2.1 HoneyD . . . 23
2.3.2.2 Dionaea . . . 23
2.3.2.3 Kippo . . . 23
2.3.2.4 Glastopf . . . 23
2.3.3 Deception using Honeypot . . . 24

SWISS GERMAN UNIVERSITY

2.4 Counter Deception 25
2.5 Fingerprinting 27
2.5.1 Active Fingerprinting 27
2.5.2 Passive Fingerprint 27
2.5.3 Fingerprinting Tools 28
2.6 Threat Modeling 29
2.7 Related Works 30

3 RESEARCH METHODOLOGY 33
3.1 Methodology Overview 33
3.2 Research Framework 34
3.2.1 Threat Modeling Process 35
3.2.2 Fingerprinting Methodology 36
3.3 Design and Experiment 37
3.4 Expert Review 38

4 EXPERIMENT RESULTS 39
4.1 Experiment Setup 39
4.2 Experiment Scenario 39
4.3 Threat Modeling 40
4.3.1 Honeypot Threat Analysis 41
4.4 Attacks Demonstration 41
4.4.1 General Honeypots 41
4.4.1.1 Layer 2 42
4.4.1.1.1 Suspicious Environment 42
4.4.1.2 Layer 4 43
4.4.1.2.1 Suspicious open ports 43
4.4.2 HoneyD 44
4.4.2.1 Layer 7 44
4.4.2.1.1 HoneyD IIS Directory Traversal Exploit . . 44
4.4.2.1.2 HoneyD HTTP Service 44
4.4.3 Dionaea 46
4.4.3.1 Layer 7 46
4.4.3.1.1 Dionaea Configuration Services 46
4.4.4 Kippo 47
4.4.4.1 Layer 7 47
4.4.4.1.1 Kippo Regex Ping Problem 47
4.4.5 Glastopf 48

SWISS GERMAN UNIVERSITY

4.4.5.1 Layer 7 48
4.4.5.1.1 Glastopf LFI Fingerprinting 48
4.4.6 Honeypot Fingerprint Overview 48
4.5 Possible Enhancements 49
4.5.1 General Honeypots 49
4.5.1.1 Layer 4 49
4.5.1.1.1 Suspicious open ports Enhancement 49
4.5.2 HoneyD 49
4.5.2.1 Layer 7 52
4.5.2.1.1 HoneyD IIS Exploit Enhancement 52
4.5.2.1.2 HoneyD HTTP Service Enhancement . . . 52
4.5.3 Dionaea 53
4.5.3.1 Layer 7 53
4.5.3.1.1 Dionaea FTP Fix 53
4.5.3.1.2 Dionaea SMBD Fix 55
4.5.3.1.3 Dionaea MS-SQL Fix 56
4.5.4 Kippo 57
4.5.4.1 Layer 7 57
4.5.4.1.1 Kippo Regex Ping Enhancement 57
4.5.5 Glastopf 57
4.5.5.1 Layer 7 57
4.5.5.1.1 Glastopf LFI Fingerprinting Enhancement . 57
4.6 Verification 58
4.6.1 General Honeypots 58
4.6.1.1 Layer 4 58
4.6.1.1.1 Suspicious Open Ports Verification 58
4.6.2 HoneyD 59
4.6.2.1 Layer 7 59
4.6.2.1.1 HoneyD ISS Exploit Validation 59
4.6.2.1.2 HoneyD HTTP Service Validation 59
4.6.3 Dionaea 61
4.6.3.1 Layer 7 61
4.6.3.1.1 Dionaea Fixes Overview 61
4.6.4 Kippo 62
4.6.4.1 Layer 7 62
4.6.4.1.1 Kippo Regex Ping Verification 62
4.6.5 Glastopf 63

SWISS GERMAN UNIVERSITY

4.6.5.1 Layer 7 63
4.6.5.1.1 Glastopf LFI Fixes 63
4.6.6 Honeypot Fixes Overview 64
4.7 Expert Review 64
4.8 Expert Review Results 65
4.8.1 #1 Expert Analysis 65
4.8.1.1 #1 Expert Discussion 66
4.8.2 #2 Expert Analysis 66
4.8.2.1 #2 Expert Discussion 67
4.8.3 Expert Review Analysis 67
4.8.4 Expert Review Conclusion 69

5 CONCLUSION AND FUTURE WORK 70
5.1 Conclusions 70
5.2 Recommendation 70
5.3 Future Work 71

GLOSSARY 72

REFERENCES 76

APPENDICES 76

A 77
A.1 HoneyD Full Comparison Table 77

B 79
B.1 #1 Expert Review 79

C 81
C.1 #1 Expert Review 81
C.1.1 Analisa 66.96.252.39 81
C.1.2 Analisa 66.96.252.46 82

PAPER 88

CURRICULUM VITAE 94

SGU ® SWISS GERMAN UNIVERSITY