An Optimized Low-Level Interaction Glastopf Honeypot for Accurate Detection of Fake Honeypot using OMNET++ Simulation

Abimbola Basiru OWOLABI
LCU/PG/002388

Being a PhD Thesis Submitted to the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria

In Partial Fulfillment of the Requirements for the Award of Doctor of Philosophy Degree (PhD) in Computer Science

2023

Certification

This is to certify that **Abimbola Basiru OWOLABI** with matriculation number **LCU/PG/002388** carried out this research work titled "**An Optimized Low-Level Interaction Glastopf Honeypot for Accurate Detection of Fake Honeypot using OMNET++ Simulation"** in the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo state, for the award of Doctor of Philosophy Degree (PhD) in Computer Science and that this has not been previously submitted.

Dr. Wumi Ajayi
(Supervisor)

Date

Dr. Wilson Sakpere
(Head of the Department)

Date

Dedication

This research work is dedicated to **Almighty God**, the creator of heaven and earth, the architect of knowledge, wisdom and understanding. And in memory of my caring and loving late father **Titiloye Ibrahim OWOLABI (Mr.)** (Easy, the Mathematician). May his soul continue to rest and bestowed with unending peace in the right hand of the Almighty Allah. Amen

Acknowledgments

My immeasurable thank goes to Almighty God, the Alpha and Omega, the beginning and the ending, for making it possible to start and end this programme of my life-time dream with joy. God, what else can I say than to devote the remaining part of my life to serve you and use the knowledge acquired for the good of mankind.

Let me sincerely express my unreserved appreciation to the management of Lead City University (LCU) Ibadan for creating enabling environment in carrying out my PhD research work.

I also acknowledged the management of Lead City University Ibadan Library, National Open University of Nigeria e-resource center, Commonwealth of Learning (COL) Open Educational Resources (OER) Centre and several e-resource platforms for allowing me to make use of their resources throughout the period of carrying out the research work.

My special appreciation goes to my HOD of Computer Science Dr Wilson Sakpere for his support and special roles played through the period of my PhD programme. You are a very peaceful and kind-hearted man, God mercies will never elude you and your home, thank you very much for being there for me always My special thank goes to my supervisor who doubled as my academic advisor, a kind hearted man, my benefactor and mentor, a man that will always correct you with love, Dr. Wumi Ajayi, I pray that God Almighty will continue to be with you and answer all your prayers. I also thank my Post graduate coordinator, Dr. Waheed for his constant and persistent guide throughout the programme, His coordination acumen is perfect, I enjoyed having you as our coordinator sir. God will perfect all that concerns you sir. I want to thank all other lecturers in the department of Computer science that have made one input or the other in the course of my PhD programme, like Prof. Akinola, Dr. Akpampa, the Secretary of the Post graduate school, Dr. Ayoade, Mrs. Dewole and my co students, may the almighty God be with you always.

I also thank my friends, co-PhD students for the knowledge shared together during the programme, also to my colleagues in office for their prayer for me always, may almighty God

never forsake you all and meet you at the point of your needs. I alone stand responsibility for the errors, if any, found in the work

Let me extend my special thanks to the love of my life, my wife, mother of my children, my jewel, my everything, Mrs. Folasade Christianah Owolabi for her support always and enduring with me throughout the period of my PhD programme. You are a wonderful, caring and lovely wife, I will forever love and care for you and never to undermine your important roles in my life. My special thanks also go to my children for supporting and enduring with me always. Adeola, Aderinsola, Adebowale, and Adedamola, you are too dear to me always my children.

"Even though the above-mentioned institutions and persons have assisted in the process of this research work, I alone stand responsibility for the errors, if any found in the work".

Thank you all and God bless.

Abimbola Basiru Owolabi

Table of Contents

Chapter Two: Literature Review

List of Tables

List of Figures

List of Acronyms

Abbreviation	Meaning
ABAC	Attribute Bases Access Control
AD	Activities Downloader
AD	Active Directory
ADT	Advanced Persistent Threat
AITP	Association of Information Technology Professionals
ANN	Artificial Neural Network
APT	Advanced Persistent Threat
ARMER	Accessible, Realistic, Measurable, Ethical, And Robust
ASCII	American Standard Code Information Interchange
BFH	Bot Finder Honeypot
BOF	Back Officer Friendly
BYOD	Bring Your Own Device
CEO:	Chief Executive Officer
CISO	Chief Information Security Officer
CL	Clients
CLUES	CLUstering of Energy
CS	Cloud Server
CSI	Cyber Security Institute
CSS	Cross-Site Scripting
CTMS	Cyber Threat Monitoring System
DAC	Discretionary Access Control

DDos	Distributed Dos Attack
DFD	Data Flow Diagram
DM:	Data Module
DMZ	De-militarized Zone
Dos	Denial of Service
DTK	Deception Tool Kit
DVM	Dalvik Virtual Machine
EHR	Electronic Health Records
ELK	Elasticsearch, Logstash, And Kibana
FH	Fake Honeypot
FHD	Fake Honeypot Detector
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HIHAT	High Interaction Honeypot Analysis Toolkit
HonSSh	Honeypot Secure Shell
HS	Honeypot Sensor
HTTP	Hyper Text Transfer Protocol
IaaS:	Infrastructure as a Service
ICS	Industrial Control System
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System

ISSA	Information Systems Security Association
MAC	Media Access Control
MAC	Mandatory Access Control
MDM:	Mobile Device Management
MITM	Man-In-The-Middle
MITMo	Man-In-The-Mobile
MLP	Multi-Layer Perception
MoE	Measurement of Efficiency
NDA	Non-disclosure Agreements
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
P2P	Point to Point
PCA	Principal Component Analysis
PII	Personally Identifiable Information
POS	Point of Sale
RAM	Random Access Memory
RDMS	Relational Database Management System
RM	Reactor Module
SaaS:	Software as A Service
SDLC:	Systems/Software Development Life Cycle
SDN	Software Defined Network
SDP	Software Defined Perimeter
SEO	Search Engine Optimization
SIP	Session Initiation Protocol

SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SMV	Symbolic Model Verifier
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
RBAC	Role Base Access Control
TCP	Transmission Control Protocol
TTP	Tactics, Techniques, And Procedures
UDP	Uniform Datagram Protocol
UML	Unified Modeling Language
URL	Uniform Resource Locator
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Networks
VPS	Virtual Private Network