

**AI-DRIVEN HONEYPOTS : REVOLUTIONIZING CYBERSECURITY
RESPONSE**

By
Jason Aljenova Christli
12002003

BACHELOR'S DEGREE
in
INFORMATION TECHNOLOGY
ENGINEERING AND INFORMATION TECHNOLOGY



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

Revision after the Thesis Defense on 3rd July 2024

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.

Jason Aljenova Christli



17/07/2024

Student

Date

Approved by:

Dr. Ir. Charles Lim BSc., M.Sc



17/07/2024

Thesis Advisor

Date

Joseph Andreas S.Kom., B.Eng., M.Sc.



17/07/2024

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium S.Kom M.Sc

Dean

Date

Jason Aljenova Christli

ABSTRACT

AI-DRIVEN HONEYPOTS: REVOLUTIONIZING CYBERSECURITY RESPONSE

By

Jason Aljenova Christli

Dr. Ir. Charles Lim BSc., M.Sc, Advisor

Joseph Andreas S.Kom., B.Eng., M.Sc., Co-Advisor

SWISS GERMAN UNIVERSITY

This thesis presents a novel approach to cybersecurity by developing honeypots enhanced with the LLaMA-3 model. These honeypots aim to revolutionize threat detection through dynamic and interactive capabilities. Traditional honeypots are often easily identified and bypassed by skilled attackers. To address this, the research focuses on creating sophisticated decoy systems capable of engaging attackers for extended periods. By leveraging LLaMA-3 for real-time, adaptive interactions, this study enhances the realism and efficacy of honeypots and deepens our understanding of attacker methodologies. The integration of advanced AI into honeypot frameworks was evaluated using the Levenshtein distance to measure response similarity between the honeypot and a real system. Results showed significant improvement in the honeypot's ability to mimic real system behaviors, particularly for basic system information and user interaction commands. However, limitations such as the lack of persistent memory and areas for improvement in command coverage were identified. Future work should focus on implementing persistent memory, expanding command coverage, utilizing different AI models, and fine-tuning models for enhanced response realism. This research represents a significant advancement in the application of AI for cybersecurity, offering a promising path to improve threat detection, analysis, and understanding of cyber threats through prolonged attacker engagement.

Keywords: Artificial Intelligence, Cybersecurity, Honeypots, LLaMA-3, Adaptive Systems, Response

© Copyright 2024
By Jason Aljenova Christli
All rights reserved

DEDICATION

This thesis is dedicated to my beloved family, whose unwavering support and love have been my constant source of strength and inspiration. Their belief in my abilities and their sacrifices have paved the way for my achievements. This work stands as a testament to their enduring patience, encouragement, and unconditional love. To them, I extend my deepest gratitude and love, for they are the foundation upon which my dreams are built and realized.

ACKNOWLEDGEMENTS

I wish to express my deepest gratitude to the members of my committee for their invaluable support, guidance, and encouragement throughout my research.

I would like to extend my sincere thanks to Dr. Ir. Charles Lim, BSc., M.Sc., my thesis advisor, for his expert advice, insightful feedback, and unwavering support. His guidance was instrumental in shaping the direction and quality of my research.

I am also profoundly grateful to Joseph Andreas S.Kom., B.Eng., M.Sc., my thesis co-advisor, for his constructive criticism, motivation, and for always being available to discuss and improve my work. His expertise greatly enhanced the outcome of this thesis.

Special thanks to Yevonnael Andrew, Dr. Charles Lim's previous research assistant, who provided invaluable assistance and support throughout the development of this thesis.

I would like to acknowledge the support and resources provided by Swiss German University. Their assistance was crucial in the successful completion of my research.

Lastly, I want to thank my family and friends for their endless support and encouragement. Their patience and understanding allowed me to focus and persevere through the challenges of my research.

Jason Aljenova Christli

TABLE OF CONTENTS

STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	5
ACKNOWLEDGEMENTS	6
CONTENTS	11
LIST OF FIGURES	12
LIST OF TABLES	13
1 INTRODUCTION	14
1.1 Research Background	14
1.2 Research Problem	16
1.3 Research Objective	17
1.4 Research Question	17
1.5 Hypothesis	17
1.6 Research Scope	18
1.7 Research Limitation	18
1.8 Document Structure	19
2 LITERATURE REVIEW	20
2.1 Current Cybersecurity Landscape	20
2.1.1 The Advent of the Internet	20
2.1.2 Evolution of the Internet and Remote System Management	20
2.2 The Role of SSH in Remote Access	21
2.2.1 SSH Protocol Overview	21
2.2.2 SSH Commands	22
2.2.3 Linux Command Categories	23
2.3 Cyber Attacks Targeting SSH	24
2.3.1 Evolution of SSH-related Cyber Threats	24

2.3.2	Traditional Security Mechanisms for SSH	25
2.3.3	Limitations of Traditional Security Mechanisms	25
2.3.4	The Rise of Cyber Deception	26
2.3.5	Honeypots as a Key Example of Cyber Deception	26
2.4	Honeypots in Cybersecurity	27
2.4.1	History of Honeypots	27
2.4.2	Types of Honeypots Based on Interaction Level	28
2.4.2.1	Low-Interaction Honeypots	29
2.4.2.2	Medium-Interaction Honeypots	30
2.4.2.3	High-Interaction Honeypots	30
2.4.3	Limitations of Traditional Honeypots	30
2.4.4	Enhancing Honeypots with AI	32
2.4.4.1	Role of AI in Cybersecurity	32
2.4.4.2	AI-driven Honeypots: Mechanisms and Benefits . . .	32
2.4.4.3	Case Studies and Examples	33
2.4.5	AI-driven Honeypots for Realistic SSH Responses	33
2.4.5.1	Importance of SSH in Cybersecurity	33
2.4.5.2	Enhancing SSH Honeypots with AI	34
2.4.5.3	Case Studies and Implementation	34
2.5	Application of AI in Cybersecurity	34
2.5.1	History of AI in Cybersecurity	34
2.5.2	Development and Evolution of AI Technologies	35
2.5.2.1	1950s-1960s: Foundational Work	35
2.5.2.2	1970s-1980s: The Rise of Expert Systems	35
2.5.2.3	1990s-2000s: Machine Learning and Data-Driven Ap- proaches	35
2.5.3	2010s: The Era of Deep Learning	36
2.5.4	2020s: Transformers and Large Language Models	36
2.5.5	Limitations of Early AI Implementations in Cybersecurity . . .	36
2.5.6	Advances in AI: From Traditional AI to Large Language Mod- els (LLMs)	36
2.5.7	The Role of LLMs in Enhancing Cybersecurity Measures . . .	37
2.6	Overview of LLM	37
2.6.1	Introduction to LLMs	37
2.6.2	Historical Development of LLMs	37

2.6.3	Transformers and Their Impact	38
2.7	Comparative Analysis of Leading LLMs	40
2.8	Tools and Methodologies for Honeypot Development	45
2.8.1	Paramiko: Python for SSH	45
2.8.2	Overview of Secure SDLC	45
2.9	Related Works & Summary	46
3	RESEARCH METHODS	49
3.1	Introduction	49
3.2	Task 1: Honeypot Development Using the SDLC Waterfall Model . . .	49
3.2.1	Overview of SDLC Waterfall Model	49
3.2.2	Phases of the Waterfall Model	50
3.2.2.1	Requirements	50
3.2.2.1.1	Objectives	50
3.2.2.1.2	Functional Requirements	50
3.2.2.1.3	Non-functional Requirements	50
3.2.2.1.4	Constraints	50
3.2.2.1.5	Risk Assessment	51
3.2.2.2	System Design	51
3.2.2.3	Initialization Process	53
3.2.2.4	Ongoing Interaction Loop	53
3.2.2.5	Implementation	54
3.2.2.5.1	Setting Up the SSH Honeypot with Paramiko	54
3.2.2.5.2	Integrating LLaMA-3 AI Model	55
3.2.2.5.3	Data Logging and Storage	55
3.2.2.5.4	Testing and Validation	56
3.2.2.6	Testing	56
3.2.2.7	Deployment	57
3.2.2.8	Maintenance	58
3.3	Task 2: Honeypot Testing Using Single Command Similarity	58
3.3.1	Command Categories	58
3.3.2	Control Environment Details	58
3.3.3	Execution Process	59
3.3.4	Data Collection	59
3.3.5	Analysis Tools	59

3.3.5.1	Evaluation Criteria	60
3.4	Summary	60
4	Experimental Results	61
4.1	Introduction	61
4.2	Honeypot Functionality Testing	61
4.2.1	Testing Setup	62
4.2.2	Results of Functionality Testing	62
4.2.3	Summary of Functionality Testing	63
4.3	Evaluation Metrics and Similarity Calculations	63
4.3.1	System Commands	63
4.3.2	Filesystem Commands	64
4.3.3	Connectivity Commands	65
4.3.4	Figures for Each Command Category	65
4.4	Analysis of Results	65
4.4.1	Overall Effectiveness	65
4.4.2	Areas of High Performance	66
4.4.3	Areas Needing Improvement	67
4.4.4	Implications for Future Development	67
4.5	Case Studies	68
4.5.1	Case Study 1: System Information Query	68
4.5.2	Case Study 2: File System Exploration	68
4.5.3	Case Study 3: Network Diagnostics	69
4.6	Limitations	70
4.6.1	Lack of Persistent Memory	70
4.6.2	Incomplete Command Coverage	70
4.6.3	Limited Dynamic Response Generation	70
4.6.4	Resource Constraints	70
4.6.5	Testing Environment Limitations	71
5	Conclusion and Recommendation	72
5.1	Conclusion	72
5.2	Future Works & Recommendations	72
5.2.1	Implementing Persistent Memory	73
5.2.2	Expanding Command Coverage	73
5.2.3	Utilizing Different AI Models	73

5.2.4	Fine-Tuning AI Models	73
5.2.5	Enhancing Dynamic Response Generation	73
5.2.6	Addressing Resource Constraints	74
5.2.7	Testing in Real-World Environments	74
GLOSSARY		75
REFERENCES		83
APPENDICES		63
A Appendix A: Installation Instructions		84
Appendix A: Installation Instructions		84
A.1	Setting up Jupyter Notebook	84
A.2	Installing Dependencies	84
A.3	Setting Up Paramiko	84
A.4	Developing the Emulated System Shell	85
A.5	Integrating LLaMA-3 AI Engine	85
A.6	Setting up the Server Environment	85
A.7	Deploying the Honeypot Application	86
A.8	Maintenance	87

List of Figures

1.1 IBM Cyber Threat Landscape 2019-2023 (IBM X-Force, 2023) 14

2.1 Types of Honeypot Based on Interaction Level (Franco et al., 2021) . . . 29

3.1 Software Development Life Cycle Waterfall 49

3.2 Overview of the honeypot’s system architecture 51

3.3 Honeypot Flowchart 52

4.1 Initial setup of the honeypot showing successful execution and response
generation from the AI model. 62

4.2 Execution of SSH commands within the honeypot environment. 62

4.3 Generation of log files capturing command execution and responses. . . 63

List of Tables

2.1 Comparison of Leading LLMs 41

2.2 Comparison of Licensing Information for Various LLM Models 42

2.3 Comparison of Related Works 48

4.1 Comparison of System Command Outputs 64

4.2 Comparison of Filesystem Command Outputs 64

4.3 Comparison of Connectivity Command Outputs 65