

LAPORAN SKRIPSI

ANALISIS SERANGAN SIBER DENGAN ALGORITMA NAÏVE BAYES UNTUK MENDETEKSI SERANGAN BRUTE FORCE ATTACK BERDASARKAN DATA LOG DARI HONEYPOT COWRIE

(Studi Kasus : PT. Riwtech Workshop Indonesia)



Disusun Oleh :

Arya Adhari Prasetyo

2020230001

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS DARMA PERSADA**

2024

LEMBAR BIMBINGAN SKRIPSI



UNIVERSITAS DARMA PERSADA

Jl. Taman Malaka Selatan, Pondok Kelapa, Jakarta Timur, Indonesia 13450
Telp. (021) 8649051, 8649053, 8649057 Fax. (021) 8649052
E-mail : humas@unsada.ac.id Home page : <http://www.unsada.ac.id>

Instrumen Bimbingan Skripsi Program Studi Teknologi Informasi Periode 2023/2024 Genap

NIM : 2020230001
Nama : Arya Adhari Prasetyo
Judul Skripsi : Analisis Serangan Siber dengan Algoritma Naive Bayes untuk Mendeteksi Serangan Brute Force Attack Berdasarkan Data Log dari Honeypot Cowrie
Dosen Pembimbing : HERIANTO, S.Pd., M.T.

No	BAB Utama Skripsi dan BATAS WAKTU Bimbingan	Materi Yang dibahas saat Konsultasi	Tanggal Bimbingan	TTD Dosen
1		Awal Paragraf 1 cm take out point lokasi penelitian Metode algoritma	17 April 2023	
2	BAB I PENDAHULUAN (15 April 2024 s.d 19 April 2024)	Lowline 2,3,3 Referensi Paragraf 1 cm	18 April 2023	
3	Paling lama upload: 19 April 2024	Point Metode Penelitian Pengumpulan Data Pengembangan Sistem	18 April 2023	
		Tanggal BAB I di ACC pembimbing =>	18/4/2024	
4	BAB II LANDASAN TEORI (22 April 2024 s.d 3 Mei 2024)	Fort 12 for All Hacking Buku 12/4/ All Hacking New Formur Table Mendeky	29 April 2024	
5		Format table All Distore Med black frame Add UML	30 April 2024	
6	Paling lama upload : 3 Mei 2024	Format Rumus 2,3 Rumus Cukur Molex	30 April 2024	
		Tanggal BAB II di ACC pembimbing =>	2/5/24	
7	BAB III ANALISA DAN PERANCANGAN / METODOLOGI (6 Mei 2024 s.d 17 Mei 2024)	Restructure Layout based on Buku panduan	13 May 2024	
8		Diagram hasil perancangan sistem penelitian Buatlah Kebutuhan Data Sub-bab Rancangan UML Rancangan DB Rancangan CRISP-DM	15 May 2024	
9	Paling lama upload : 17 Mei 2024	Perubahan Andara kebutuhan ke CRISP-DM	17 May 2024	
		Tanggal BAB III di ACC pembimbing =>	17-5-24	



UNIVERSITAS DARMA PERSADA

Jl. Taman Malaka Selatan, Pondok Kelapa, Jakarta Timur, Indonesia 13450
Telp. (021) 8649051, 8649053, 8649057 Fax. (021) 8649052
E-mail : humas@unsada.ac.id Home page : <http://www.unsada.ac.id>

10		• Dashboard Interface perlu di Percontik	23/5/24	
11	Percobaan Demo Aplikasi atau Sistem (20 Mei 2024 s.d 31 Mei 2024)	• Pikirkan Lebih dalam, terkait Data Preprocessing, tawarlah		
12		Labeling Section		
13	Paling lama upload : 31 Mei 2024	• Perkuat Dasar knowledge terkait proyek Skripsi		
		Tanggal Aplikasi/Sistem ACC pembimbing =>	4/6/2024	
14	BAB IV HASIL DAN PEMBAHASAN (3 Juni 2024 s.d 14 Juni 2024)	• Poin Ciri perlu ke : counter 10 • Dugaan puitika foto kandi		
15				
16	Paling lama upload : 14 Juni 2024			
		Tanggal BAB IV di ACC pembimbing =>	20-6-24	
17	BAB V PENUTUP (17 Juni 2024 s.d 19 Juni 2024)			
18	Paling lama upload : 19 Juni			
		Tanggal BAB V di ACC pembimbing =>	21-6-24	

Catatan :

- Mahasiswa harus konsultasi jauh-jauh hari sebelum batas akhir tanggal per BAB nya.
- Tanggal Bimbingan dan ACC per BAB **JIARUS** sebelum batas tanggal maksimum, tetapi boleh sebelum tanggalnya jika bisa lebih cepat
- Dokumen ini **WAJIB** diupload ke gform yang ditentukan pada range tanggal setiap BAB
- Ujian Seminar ISI akan diadakan pada range tanggal : 24 s.d 28 Juni 2024

Di Acc untuk Seminar Isi, pada tanggal : 21-6-24

Oleh Dosen Pembimbing Skripsi

LEMBAR REVISI



UNIVERSITAS DARMA PERSADA

Jl. Taman Malaka Selatan, Pondok Kelapa, Jakarta Timur, Indonesia 13450

Telp. (021) 8649051, 8649053, 8649057 Fax. (021) 8649052

E-mail : humas@unsada.ac.id Home page : <http://www.unsada.ac.id>

LEMBAR REVISI - SIDANG SKRIPSI

NIM>Nama : 2020230001 - Arya Adhari Prasetyo
Fakultas/Prodi : Teknik / Teknologi Informasi

No.	Keterangan Revisi	Dosen

Mengerahui,

Kaprodi Teknologi Informasi

Herianto, S.Pd., MT.

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Arya Adhari Prasetyo

NIM : 2020230001

Fakultas : Teknik

Jurusan : Teknologi Informasi

Menyatakan bahwa Laporan Tugas Akhir Skripsi ini saya susun sendiri berdasarkan hasil kajian literatur dan akademik terdahulu, perancangan sistem, implementasi sistem pada objek dari subjek yang diteliti, dan beberapa hasil evaluasi deployment sistem yang terkait dan relevan dengan Tugas Akhir.

Demikian pernyataan ini dibuat dengan sesungguhnya agar dapat dipergunakan untuk beberapa kepentingan yang dibutuhkan.

Jakarta Pusat, 24 Juli 2024



Arya Adhari Prasetyo

LEMBAR PENGUJI LAPORAN SKRIPSI

Laporan Skripsi yang berjudul:

**ANALISIS SERANGAN SIBER DENGAN ALGORITMA NAÏVE BAYES UNTUK
MENDETEKSI SERANGAN BRUTE FORCE ATTACK BERDASARKAN DATA
LOG DARI HONEYPOT COWRIE**

(Studi Kasus : PT. Riwtech Workshop Indonesia)

telah diajukan pada hari/tanggal :

Rabu, 24 Juli 2024

Penguji 1


(Herianto, S.Pd., M.T)

Penguji 2


(Adam Arif Budiman. ST, M.Kom)

Penguji 3


(Muhammad Zacky Asy'ari, S.T., MSc&T)

LAMPIRAN LEMBAR PENGUJI LAPORAN SKRIPSI
SURAT KETERANGAN PENELITIAN



ENGINEERING, CONSTRUCTION, MACHINING, MOVERS,
MECHANICAL, LIFTING, ELEVATOR
JL. BINTARA 14 NO. 84 BEKASI TELP : 02189494244 PHONE : 0812-2447-5419 / 0851-9879-9609
EMAIL : riwtech@gmail.com Web : Riwtech.com

SURAT KETERANGAN

Dengan hormat,

Saya selaku Admin Staff dari PT. Riwtech Workshop Indonesia, memberikan izin kepada :

Nama : Arya Adhari Prasetyo
NIM : 2020230001
Asal Instansi : Universitas Dharma Persada
Program Studi : Teknologi Informasi
Objek : Seminar & Sidang Akhir Skripsi

Untuk melaksanakan penelitian dan melakukan simulasi atas suatu penelitian tugas akhir dengan judul : **"Analisis Serangan Siber dengan Algoritma Naïve Bayes untuk Mendeteksi Serangan Brute Force Attack berdasarkan Data Log dari Honeypot Cowrie"** . Saya juga mengizinkan mahasiswa untuk melakukan simulasi penerapan teknologi terkait pada *staging-env* dan bukan pada *production-env* agar tidak mengganggu operasional dan proses bisnis yang ada.

Demikian surat keterangan dan perizinan ini disampaikan agar dapat dipergunakan sebagaimana mestinya.

Bekasi, 11 Juli 2024

Admin Staff Perusahaan


TECH
ORKSHOP
(Ibu Endang Sugianti)

LEMBAR PENGESAHAN

**ANALISIS SERANGAN SIBER DENGAN ALGORITMA NAÏVE BAYES
UNTUK MENDETEKSI SERANGAN BRUTE FORCE ATTACK
BERDASARKAN DATA LOG DARI HONEYPOT COWRIE**

(Studi Kasus : PT. Riwtech Workshop Indonesia)

Disusun oleh:

Arya Adhari Prasetyo

2020230001



Endah Sugiarti

Pembimbing Lapangan

Herianto, S.Pd., M.T

Pembimbing Laporan

Herianto, S.Pd., M.T

Kajur Teknologi Informasi

KATA PENGANTAR

Bismillahirrahmanirrahim,

Assalamu'alaikum Warahmatullahi Wabarakatuuh.

Dengan segala kerendahan hati, Penulis panjatkan rasa syukur dalam kehadiran Allah SWT. yang telah memberikan limpahan rahmat dan karunia-Nya yang berupa kemampuan daya pikir, kesehatan jasmani dan rohani, dan juga sebuah kesempatan pada penulis, untuk menyelesaikan Laporan Skripsi sebagai Tugas Akhir yang berjudul **“Analisis Serangan Siber Dengan Algoritma *Naïve Bayes* Untuk Mendeteksi Serangan *Brute Force Attack* Berdasarkan *Data Logs* Dari *Honeypot Cowrie*”**.

Terima kasih kepada semua pihak yang telah membantu penulis dalam proses pembuatan skripsi ini, karena berkat dorongan dan motivasi dari berbagai pihak, bantuan materil dan immaterial, ide brilian dan solutif dari berbagai mentor, Penulis dapat menyelesaikan skripsi ini dengan secara sekuensial dan structural, terucap terimakasih penulis ucapkan kepada :

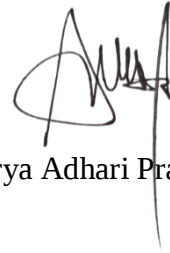
1. Allah SWT. , sebagai sandaran utama dan terakhir yang penulis percayakan semuanya atas segala kelancaran yang diberikan selama proses *concepting*, *mind mapping*, *develop*, hingga tahap *proof of concept*.

2. Ibu dan Ayah Penulis, sebagai sosok utama yang mendukung lahir dan batin agar menjadikan Penulis sebagai sosok Pembelajar yang berkomitmen dan memiliki tanggung jawab tinggi terhadap persoalan akademis.
3. Kepada Bapak HERIANTO, S.Pd., M.T. selaku Ketua Program Studi S1 Teknologi Informasi Universitas Darma Persada, dan Dosen Pembimbing Skripsi, yang karenanya Penulis dapat menyelesaikan persoalan Teknis dengan tingkat kompleksitas yang tidak sederhana, namun dengan arahan yang solutif hingga persoalan terselesaikan.
4. Bapak Adam Arif Budiman, S.T., M.Kom, Bapak Suzuki Syofian, M.Kom., Bapak Aji Setiawan, S.Kom., MMSI, Bapak Afri Yudha, M.Kom, Bapak Andi Susilo, M.T.I., Bapak Bagus Tri Mahardika, MMSI., Bapak Yan Sofyan, A.S., M.Kom., dan Bunda Timor Setiyaningsih S.T., M.T.I., selaku dosen Teknologi Informasi Universitas Darma Persada.
5. Admin Staff PT. Riwtech Workshop Indonesia, selaku pemberi perizinan untuk menggunakan lingkungan virtual sebagai simulasi dan uji coba terkait topik skripsi yang diangkat.
6. Kepada 3 Mentor dengan masing-masing bidangnya, Syifa Rizka Sagita, Shilvi Yanti Safitri, dan Diki Hamdani. Karenanya, penulis dapat mewujudkan sebuah topik dengan ‘value’ didalamnya untuk bisa diimplementasikan pada dunia industry 4.0 dalam menyempurnakan proses ‘Business Process’ yang ada.

7. Kepada teman-teman angkatan seperjuangan, Rizkhi, Yayan, dan teman-teman lainnya yang tidak dapat disebutkan satu persatu.

Akhir kata, semoga Laporan Skripsi ini bermanfaat dan memiliki nilai yang bisa dijadikan referensi pada lingkup terkait.

Jakarta Pusat, 24 Juni 2024



(Arya Adhari Prasetyo)



**ANALISIS SERANGAN SIBER DENGAN ALGORITMA
NAÏVE BAYES UNTUK MENDETEKSI SERANGAN BRUTE
FORCE ATTACK BERDASARKAN DATA LOG DARI
HONEYPOT COWRIE**

Arya Adhari Prasetyo

2020230001

Program Studi Teknologi Informasi

Universitas Darma Persada

Email : aryaadhari15@gmail.com

ABSTRAK

Serangan siber telah menjadi salah satu ancaman yang sangat signifikan dalam dunia teknologi informasi masa kini. Serangan Brute Force Attack merupakan salah satu jenis serangan siber yang paling umum terjadi terhadap layanan dengan protokol SSH. Dalam penelitian ini, dilakukan analisis serangan Brute Force Attack menggunakan algoritma Naive Bayes berdasarkan data log yang dihasilkan oleh Honeypot Cowrie. Honeypot Cowrie berperan sebagai perangkat yang meniru layanan SSH yang asli dan mencatat semua percobaan login yang dilakukan oleh penyerang. Data log yang diperoleh dari Honeypot Cowrie kemudian dianalisis menggunakan algoritma Naive Bayes untuk mendeteksi pola serangan Brute Force Attack. Metode ini memungkinkan kita untuk mengidentifikasi pola serangan yang mencurigakan dan potensial, sehingga memungkinkan pengguna untuk mengambil tindakan preventif yang sesuai dengan event yang terjadi pada private atau public network. Eksperimen dilakukan menggunakan dataset serangan siber yang diduga adalah serangan Brute Force Attack yang diperoleh dari lingkungan simulasi | virtual environment. Berdasarkan jumlah data yang didapatkan dari Honeypot Cowrie pada suatu period tertentu, dihasilkan jumlah data 39.321 raw, tingkat keberhasilan penerapan algoritma naïve bayes dalam mendeteksi serangan brute force attack berdasarkan data logs dari honeypot cowrie terbilang cukup baik, dengan data uji baru dalam range waktu yang sudah ditentukan, menghasilkan nilai evaluasi : Accuracy, Precision, Recall, dan F1-Score : 98% , 99% , 80%, dan 87%. dan hasilnya menunjukkan efektivitas algoritma Naive Bayes dalam mendeteksi serangan Brute Force Attack dengan tingkat akurasi yang memuaskan. Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan teknik deteksi Brute Force yang lebih mutakhir dan responsif.

Kata Kunci : Serangan Siber, Machine Learning, Honeypot Cowrie, Naïve Bayes, SSH Brute Force Attack

CYBER ATTACK ANALYSIS WITH NAÏVE BAYES ALGORITHM TO DETECT BRUTE FORCE ATTACK BASED ON LOG DATA FROM COWRIE HONEYPOT

Arya Adhari Prasetyo

2020230001

Information Technology Study Program

Darma Persada University

Email : aryaadhari15@gmail.com

ABSTRACT

Cyber attacks have become one of the most significant threats in the world of information technology today. Brute Force Attack is one of the most common types of cyber attacks against services with SSH protocol. In this research, the Brute Force Attack is analyzed using the Naive Bayes algorithm based on log data generated by the Cowrie Honeypot. Honeypot Cowrie acts as a trap that mimics the original SSH service and records all login attempts made by the attacker. The log data obtained from Honeypot Cowrie is then analyzed using the Naive Bayes algorithm to detect Brute Force Attack patterns. This method allows us to identify suspicious and potential attack patterns, thus enabling users to take preventive actions according to events that occur on private or public networks. Experiments were conducted using a dataset of cyber attacks suspected of being Brute Force Attack attacks obtained from a simulated virtual environment. Based on the amount of data obtained from Honeypot Cowrie in a certain period, a total of 39,321 raw data is generated, the success rate of applying the naïve bayes algorithm in detecting brute force attacks based on logs data from honeypot cowrie is quite good, with new test data in a predetermined time range, resulting in an evaluation value: Accuracy, Precision, Recall, and F1-Score: 98%, 99%, 80%, and 87%. and the results show the effectiveness of the Naive Bayes algorithm in detecting Brute Force Attack with a satisfactory level of accuracy. This research is expected to contribute to the development of more sophisticated and responsive Brute Force detection techniques.

Keywords: Cyber Attack, Machine Learning, Cowrie Honeypot, Naïve Bayes, SSH Brute Force Attack

DAFTAR ISI

KATA PENGANTAR	ix
ABSTRAK	xii
ABSTRACT	xiii
DAFTAR ISI	xiv
DAFTAR TABEL	xix
DAFTAR GAMBAR	xx
DAFTAR LAMPIRAN	xxiii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	7
1.6 Metode Penelitian	9
1.6.1 Metode Pengumpulan Data	9
1.6.2 Metode Pengembangan Sistem	9
1.7 Sistematika Penulisan Skripsi	11
BAB II	13

LANDASAN TEORI.....	13
2.1 Kajian Penelitian Terdahulu.....	13
2.2 Tinjauan Pustaka	18
2.2.1 Serangan Siber	18
2.2.2 Brute Force Attack	19
2.2.3 Lanskap Keamanan Siber Indonesia	21
2.2.4 Laporan Bulanan Publik	22
2.2.5 Secure Shell (SSH).....	25
2.2.6 Honeypot	26
2.2.7 Low-Interaction Honeypot	27
2.2.8 Medium-Interaction Honeypot	27
2.2.9 High-Interaction Honeypot.....	27
2.2.10 Honeypot Cowrie (Medium-Interaction Honyepot)	28
2.2.11 Data Log	29
2.2.12 Algoritma Naïve Bayes	30
2.2.13 Kelebihan dan Kekurangan Naïve Bayes	31
2.2.13.1 Kelebihan Algoritma Naïve Bayes	31
2.2.13.2 Kekurangan Algoritma Naïve Bayes	32
2.2.14 Tipe Algoritma Naïve Bayes	32
2.2.14.1 Naïve Bayes Classifier	33
2.2.14.2 Multinomial Naïve Bayes	33

2.2.14.3 Gaussian Naïve Bayes Classifier	33
2.2.15 Evaluasi Kinerja Model.....	34
2.2.15.1 Confusion Matrix.....	34
2.2.15.2 Accuracy	36
2.2.15.3 Precision.....	36
2.2.15.4 Recall	36
2.2.15.5 F-1 Score	36
2.2.16 CRISP-DM (Cross-Industry Standard Process for Data Mining).....	37
2.2.17 Virtual Environtment – Virtualisasi Server	39
2.2.18 Penetration Testing Technic	41
2.2.19 Penetration Tools	42
2.2.19.1 Hydra.....	43
2.2.19.2 Medusa.....	43
2.2.19.3 Ncrack.....	43
2.2.20 Pemodelan UML	43
2.2.20.1 UML Use Case Diagram.....	43
2.2.20.2 UML Activity Diagram.....	45
BAB III METODOLOGI PENELITIAN.....	48
3.1 Rancangan Dasar Penelitian.....	48
3.1.1 Bidang dan Jenis Penelitian	48
3.1.2 Lokasi Penelitian.....	48

3.1.3 Jadwal Penelitian	49
3.2 Rancangan Metodologi Penelitian.....	51
3.2.1 General Blueprint	51
3.2.2 Perancangan UML	53
3.2.2.1 Rancangan Use Case Diagram	53
3.2.2.2 Rancangan Activity Diagram	55
3.2.3 Rancangan Struktur Database	59
3.2.4 Rancangan Interface Aplikasi.....	59
3.2.5 Analisa dan Perancangan Tahap CRISP-DM.....	62
3.2.5.1 Analisa Tahap Business Understanding.....	62
3.2.5.2 Analisa Tahap Data Understanding	63
3.2.5.3 Rancangan Tahap Data Preparation.....	64
3.2.5.4 Rancangan Tahap Pemodelan	67
3.2.5.5 Rancangan Tahap Testing	69
3.2.5.6 Rancangan Tahap Deployment	70
BAB IV	72
4.1 Hasil Penelitian	72
4.1.1 Spesifikasi Hardware dan Software Yang Digunakan	72
4.1.1.1 Software Requirement	72
4.1.1.2 Hardware Requirement	73
4.1.2 Tampilan Interface Hasil Deploy	74

4.1.2.1 Login Page	74
4.1.2.2 Home Page	76
4.1.2.3 Predict Page.....	77
4.1.3 Struktur Database	86
4.2 Analisa Hasil	88
4.2.1 Percobaan Input-Output	88
4.2.1.1 Extract Logs Testing.....	88
4.2.1.2 Preprocess Data Testing.....	91
4.2.1.3 Predict Data Test	94
4.2.2 Testing Hasil.....	99
4.2.3 Modifikasi atau Optimalisasi Dari Sistem Terdahulu	102
4.2.4 Proses Deploy Sistem Aplikasi.....	105
4.2.4.1 Honeypot Cowrie Deployment.....	105
4.2.4.2 AI Modal Deployment	110
BAB V.....	126
5.1 Kesimpulan	126
5.2 Saran	127
DAFTAR PUSTAKA	129
LAMPIRAN	132

DAFTAR TABEL

Tabel 2. 1 Tinjauan Referensi Penelitian Terdahulu.....	13
Tabel 2. 2 Confusion Matrix Table	35
Tabel 2. 3 UML Use Case Diagram	43
Tabel 2. 4 UML Activity Diagram.....	45
Tabel 3. 1 Jadwal Penelitian	49
Tabel 3. 2 Database Users.....	59
Tabel 4. 1 Software Package Requirement	72
Tabel 4. 2 Hardware Requirement.....	73
Tabel 4. 3 Input-Output Summarize	97
Tabel 4. 4 Evaluasi Modal	99
Tabel 4. 5 Evaluasi Predict	100
Tabel 4. 6 Komparasi Sistem Terdahulu dengan Sistem Yang Dibangun...	102

DAFTAR GAMBAR

Gambar 2. 1 Brute Force Attack.....	20
Gambar 2. 2 Trafik Anomali Serangan Siber di Indonesia Tahun 2023	22
Gambar 2. 3 Laporan Bulanan Publik Bulan Agustus 2023	23
Gambar 2. 4 Top 5 Sumber IP Anomali	23
Gambar 2. 5 Sebaran Jenis Sektor Terindikasi Mengalami Dugaan Indikasi Insiden Keamanan Siber	24
Gambar 2. 6 Cowrie JSON Log Sample	29
Gambar 2. 7 CRISP-DM	37
Gambar 2. 8 Virtual Environtment.....	41
 Gambar 3. 1 General Blueprint.....	 52
Gambar 3. 2 Penetration Testing Schema.....	53
Gambar 3. 3 Staging Environtment Use Case	54
Gambar 3. 4 AI Local Server	55
Gambar 3. 5 Staging Environtment Login Section.....	56
Gambar 3. 6 Honeypot Cowrie Deployment and Data Extraction	57
Gambar 3. 7 AI Local Environtment Activity	58
Gambar 3. 8 Login Page	60
Gambar 3. 9 Overview Page	60
Gambar 3. 10 Modal.....	61
Gambar 3. 11 Report/History	62
Gambar 3. 12 Honeypot Cowrie JSON Log.....	64

Gambar 3. 13 Data Extraction	65
Gambar 3. 14 Honeypot Cowrie Data Log.....	66
Gambar 3. 15 Tahap Pemodelan	68
Gambar 3. 16 Tahapan Testing.....	69
Gambar 3. 17 Tahapan Deployment	71
Gambar 4. 1 Login Page	74
Gambar 4. 2 Home Page.....	76
Gambar 4. 3 Predict Page [1]	77
Gambar 4. 4 Predict Page [2]	77
Gambar 4. 5 Extract Logs	78
Gambar 4. 6 Extract Logs Process	79
Gambar 4. 7 Cowrie's Data Logs	80
Gambar 4. 8 Preprocess Data.....	80
Gambar 4. 9 Preprocess Data.....	81
Gambar 4. 10 Preprocess Data Result	82
Gambar 4. 11 Predict.....	83
Gambar 4. 12 Predict Process	84
Gambar 4. 13 Predict Result	85
Gambar 4. 14 PhpMyAdmin	86
Gambar 4. 15 Table Structure.....	86
Gambar 4. 16 Extract Logs Testing	88
Gambar 4. 17 Validation on Invalid Input on Extract Logs	89
Gambar 4. 18 JSON Form's Data Logs Output File	90

Gambar 4. 19 Upload Max File Size Limitation	92
Gambar 4. 20 Upload JSON File to Section Preprocess Data	93
Gambar 4. 21 Download Preprocessed Data	93
Gambar 4. 22 Preprocessed Data	94
Gambar 4. 23 Upload Preprocessed Data to doing a Predicting New Data... 95	
Gambar 4. 24 Predict New Data.....	96
Gambar 4. 25 Modal Train's Confusion Matrix.....	100
Gambar 4. 26 Predict Eval's Confusion Matrix	101
Gambar 4. 27 Modal Assesment.....	104
Gambar 4. 28 Modal Evaluation without SMOTE.....	105
Gambar 4. 29 SSH Status Listen Port.....	107
Gambar 4. 30 Honeypot Cowrie's Service Status	109
Gambar 4. 31 General Perspective.....	110
Gambar 4. 32 Main Function General Perspective	125

DAFTAR LAMPIRAN

Lampiran 1 Surat Bebas Plagiarism	132
Lampiran 2 Surat Keterangan Penelitian.....	133
Lampiran 3 Hasil Turnitin	134
Lampiran 4 Source Code.....	146

