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

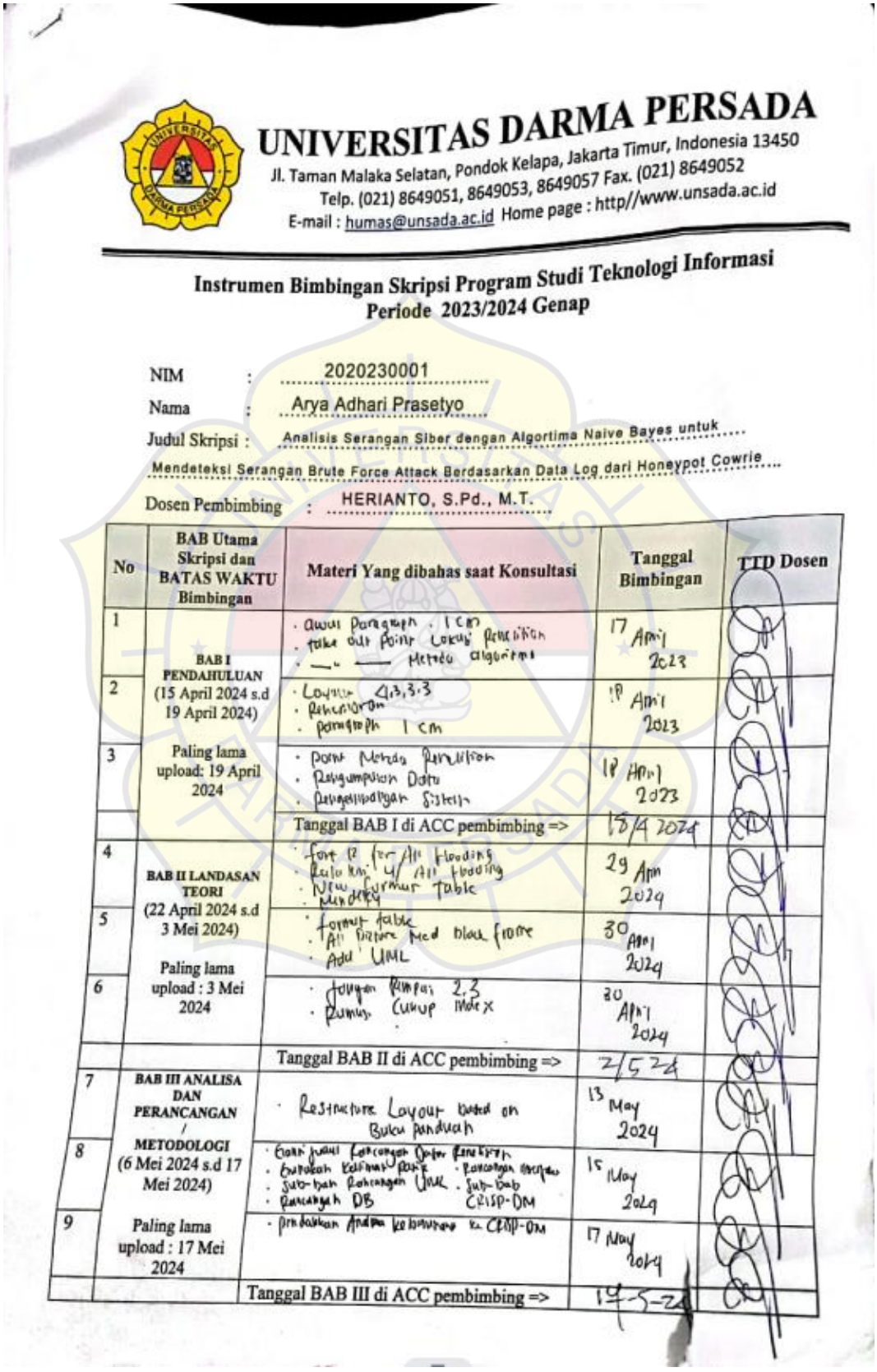
PROGRAM STUDI TEKNOLOGI INFORMASI

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 Algortima 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	BAB I PENDAHULUAN (15 April 2024 s.d 19 April 2024) Paling lama upload: 19 April 2024	· Awal paragraph . 1 cm · Take out point Lokus Penelitian · —" —— Metode algoritma	17 April 2023	
2		· Layout 4,3,3,3 · Rancangan · paragraph 1 cm	18 April 2023	
3		· Point Metode Penelitian · Pengumpulan Data · Pengembangan Sistem	18 April 2023	
		Tanggal BAB I di ACC pembimbing =>	15/4 2024	
4	BAB II LANDASAN TEORI (22 April 2024 s.d 3 Mei 2024) Paling lama upload : 3 Mei 2024	· font 12 for All Heading · Paragraf 4/ All Heading · New Format Table · Numbering	29 April 2024	
5		· format table · All Picture Need black frame · Add UML	30 April 2024	
6		· Tanggan Rumpai 2,3 · Rumus Cukup Index	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) Paling lama upload : 17 Mei 2024	· Restructure Layout based on Buku panduan	13 May 2024	
8		· Cari jurnal Perancangan Dalam Penelitian · Berdasarkan Referensi Penelitian · Perancangan Arsitek · Sub-bab Perancangan UML · Sub-bab · Rancangan DB CRISP-DM	15 May 2024	
9		· Pendasikan Analisa 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	**Percobaan Demo Aplikasi atau Sistem** (20 Mei 2024 s.d 31 Mei 2024) Paling lama upload : 31 Mei 2024	· Dashboard interface perlu di percantik	23/5/24	
11		· Pikirkan lebih dalam, terkait Data Preprocessing, tambahan		
12		Labeling Section · perkuat Dasar knowledge		
13		terkait Proses Skripsi		
		Tanggal Aplikasi/Sistem ACC pembimbing =>	4/6/2024	
14	**BAB IV HASIL DAN PEMBAHASAN** (3 Juni 2024 s.d 14 Juni 2024) Paling lama upload : 14 Juni 2024	· Pola Code perlu ke : Counter 10 · Dapat pustaka tulis tangan		
15				
16				
		Tanggal BAB IV di ACC pembimbing =>	20-6-24	
17	**BAB V PENUTUP** 17 Juni 2024 s.d 19 Juni 2024) Paling lama upload : 19 Juni			
18				
		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 HARUS 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

Hargianto

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

Mengetahui,

Ka Prodi Teknologi Informasi

Herianto, S.Pd., MT.

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Arya Adhari Prasetyo

NIM : 2020230001

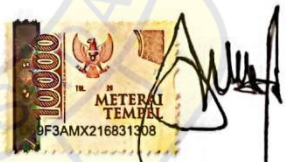
Fakultas : Teknik

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

ENGINERING, CONSTRUCTION, MACHINING, MOVERS,
MECHANICAL, LIFTING, ELEVATOR
JL.BINTARA 14 NO.84 BEKASI TELP : 02189494244 PHONE : 0812-2447-5419 / 0851-9879-9609
EMAIL :riwttech@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 Darma 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

(Ibu Endah Sugiarti)

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	**Herianto, S.Pd., M.T**
Pembimbing Lapangan	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 kehadirat 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 :

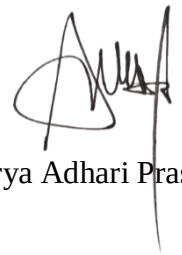
1. Allah SWT. , sebagai sandaran utama dan terakhir yang penulis percayakan semuanya atas segala kelancaran yang diberikan selama proses *concepting*, *mind mapping*, *develop*, hingga tahap *proof of concept*.

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 perangkap 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 algortima 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 environtment. Berdasarkan jumlah data yang didapatkan dari Honeypot Cowrie pada suatu period tertentu, dihasikan 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN