BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan era digital yang semakin berkembang setiap waktunya, keamanan informasi telah menjadi salah satu isu utama bagi organisasi maupun individu. Berdasarkan data statistik yang penulis riset mengenai ‘anomali trafik’, menurut Badan Siber dan Sandi Negara (BSSN), lewat Lanskap Keamanan Siber Indonesia Tahun 2023, menyebutkan bahwa total ‘trafik anomali’ di Indonesia selama tahun 2023 adalah sebesar 430.990.831 juta anomali. Anomali trafik tertinggi terjadi pada bulan Agustus 2023 dengan jumlah 78.464.385, sedangkan anomali terendah terjadi pada bulan November 2023 dengan jumlah 19.296.439 juta anomali. Aktivitas anomali trafik ini tentunya bisa berdampak pada penurunan performa perangkat dan jaringan itu sendiri, pencurian data sensitif, hingga perusakan reputasi dan penutunan kepercayaan terhadap suatu organisasi tertentu dalam memberikan suatu jasa atau *service* pada masyarakat Indonesia itu sendiri.

Berdasarkan Laporan Bulanan Agustus 2023, ada 2 jenis serangan siber terbesar yang menyumbang angka tertinggi dari aktivitas trafik anomali yang terjadi. Jenis serangan siber itu adalah SSH Account Brute Force Attack dengan jumlah trafik 2.876.228, lalu disusul oleh jenis serangan siber yang serupa, namun dengan target yang berbeda, yaitu MSSQL Database Account Brute Force Attack dengan total trafik 359.241. Lalu berdasarkan sebaran kasus per-sektor yang dilaporkan pada platform yang sama, menunjukkan bahwa sektor Administrasi

Pemerintahan menjadi sektor yang paling banyak mendapatkan penetrasi serangan siber dengan total 26 kasus, lalu pada sektor lainnya terjadi sebesar 17 kasus, yang tentunya laporan ini merupakan hasil data yang di olah berdasarkan laporan yang diterima oleh BSSN (Badan Siber dan Sandi Negara, 2023).

Serangan siber sendiri telah menjadi salah satu ancaman yang sangat berpengaruh dalam dunia teknologi informasi masa kini. Berdasarkan beberapa paparan sebelumnya, kita dapat memahami bahwa jenis serangan Brute Force Attack merupakan salah satu jenis serangan siber yang paling umum terjadi terhadap layanan dengan protocol SSH. Dalam penelitian ini, kami akan melakukan analisis serangan brute force attack menggunakan algoritma Naïve Bayes berdasarkan data log yang dihasilkan oleh Honeypot Cowrie.

SSH merupakan singkatan dari *Secure Shell*, SSH merupakan sebuah protocol keamanan berbasis pada lapisan aplikasi (application layer) yang dikembangkan oleh IETF's Network Working Group. IETF Group merupakan suatu komunitas terbuka internasional yang terdiri dari perancang jaringan, operator, vendor, dan peneliti yang bekerja pada evolusi dan operasi internet. Serangan siber SSH Brute Force Attack ini semakin meningkat dalam skema penyerangannya tiap tahunnya. Hal ini dibuktikan oleh *tools* serangan yang semakin variative dan bersifat terbuka (open source), membuat skema penyerangan siber ini menjadi beragam dan kompleks. Tentunya, hal ini menimbulkan ancaman serius terhadap integritas dan kerahasian data pada suatu organisasi tertentu. Brute force attack merupakan salah satu jenis serangan siber yang paling umum dan berbahaya, dimana seorang penyerang akan mencoba untuk mendapatkan hak akses

ke suatu service/system dengan mencoba berbagai kombinasi kata sandi dan username secara berulang hingga menemukan hak akses yang benar.

Untuk mengantisipasi jenis serangan ini, diperlukan beberapa pendekatan yang proaktif dan mutakhir dalam mendeteksi dan mencegah serangan siber ini untuk merusak internal system kita. Salah satu pendekatan yang akan penulis angkat adalah dengan menganalisa *Log* yang dihasilkan oleh Honeypot yang akan berperan sebagai *umpan* bagi para penyerang, lalu dianalisa setiap *event* yang terjadi pada *service umpan* ini dengan salah satu algoritma machine learning, yaitu Naïve Bayes.

Honeypot merupakan sebuah mekanisme sistem keamanan yang digunakan untuk membangun *cloning service* sebagai umpan bagi para *attacker* dan akan mencatat dan mengumpulkan informasi setiap aktivitas yang terjadi pada service tersebut terhadap sistem utama (Pamungkas & Sembiring, 2023). Ada berbagai jenis honeypot yang sedang dikembangkan dari berbagai organisasi. Pada dasarnya konsep honeypot yang dikembangkan adalah sama, yatiu service ini akan mencoba membangun suatu service aplikasi maupun sebuah protocol semirip mungkin dengan service utamanya. Lalu nanti seorang admin akan membiarkan service ini terlihat *terbuka* yang akan menginisiasi hacker untuk melancarakan berbagai jenis serangan. Lalu dari *event serangan* tersebut seorang admin sistem akan melakukan analisa pola serangan dan pada akhirnya bisa membantu mereka untuk menentukan *decision* yang perlu dilakukan.

Salah satu jenis honeypot yang bisa kita gunakan sebagai pendekatan yang sesuai topik yang akan penulis angkat adalah Honeyot Cowrie Medium-interaction.

Honeypot Cowrie akan membuat service SSH palsu yang sangat dibuat identic dengan server fisik yang asli, sehingga ketika nantinya para hacker berhasil menerobos masuk kedalam service ini, dilakukan semacam *monitoring* bahkan secara realtime terkait apa saja yang dikerjakan oleh si penyerang terhadap service umpan yang kita pasang pada suatu dedicated infrastruktur.

Dalam konteks ini, tidak hanya menerapkan honeypot pada suatu organisasi tertentu, melainkan digunakan salah satu Algoritma Machine Learning untuk membantu menganalisa suatu event yang terjadi, yaitu Algoritma Klasifikasi Naïve Bayes. Naïve Bayes merupakan metode pengklasifikasian probabilitas sederhana yang sesuai dengan Teorema Bayes, kemudian dikombinasikan dengan Naïve yang berarti variable *independent* (Ardyanti et al., 2020). Naïve Bayes adalah salah satu contoh metode analisis yang dapat mengklasifikasikan pola serangan (Singh, *et al.* 2020). Hal ini dibuktikan pada penelitian yang telah menerapkan metode Naïve Bayes untuk *Honeypot Dionaea* dalam Mendeteksi Serangan *Port Scanning*. Dari penelitian ini menghasilkan nilai *class label Yes* yang dilihat dari *F-Measure* berupa 0,714%. Nilai *class label No* berupa 0,909%, sehingga didapat hasil rata-rata *F-Measure* sebanyak 0,849%. Pengujian *data log* serangan *Port Scanning* dengan metode *Naïve Bayes* pada WEKA menunjukkan tingkat kesalahan klasifikasi yang kecil yaitu 13,7% dibandingkan dengan 86,2% tingkat keberhasilan. Dengan kata lain tingkat akurasi yang didapatkan lebih tinggi dibandingkan *rate error* (NURILAHI et al., 2022).

Dengan menganalisa data log dari Honeypot Cowrie menggunakan algoritma Naïve Bayes, diharapkan kita dapat mengidentifikasi pola serangan Brute Force Attack dan mengambil tindakan pencegahan yang sesuai. Oleh karena itu,

penelitian ini bertujuan untuk menyelidiki efektivitas algoritma Naïve Bayes dalam mendeteksi serangan brute force berdasarkan data log dari Honeypot Cowrie , dengan harapan dapat memberikan kontribusi yang signifikan dalam upaya perlindungan keamanan informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan diatas, penulis membuat rumusan masalah dari Studi Kasus di PT. Riwtech Workshop Indonesia adalah sebagai berikut :

1. Bagaimana efektivitas algoritma Naïve Bayes dalam mendeteksi serangan Brute Force Attack berdasarkan data log dari Honeypot Cowrie di lingkungan virtual PT. Riwtech Workshop Indonesia ?
2. Apa saja parameter atau karakteristik dari pola serangan Brtue Force Attack yang dapat diidentifikasi melalui analisis data log dari Honeypot Cowrie di lingkungan virtual PT. Riwtech Workshop Indonesia ?
3. Bagaimana tingkat keberhasilan algoritma Naïve Bayes dalam membedakan serangan Brute Force Attack dari aktvitas normal berdasarkan data log dari Honeypot Cowrie di lingkungan virtual PT. Riwtech Workshop Indonesia ?

1.3 Batasan Masalah

Batasan-batasan masalah yang akan diterapkan dalam penelitian yang penulis angkat ini adalah sebagai berikut :

1. Focus penelitian hanya pada analisis serangan siber brute force attack menggunakan algoritma naïve bayes berdasarkan data log dari honeypot cowrie
2. Karena data log serangan siber aktual dari PT. Riwtech Workshop Indonesia adalah bersifat *confidential* , maka penulis akan membuat sebuah *virtual environtment* | lingkungan virtual untuk menghasilkan data log dari jenis serangan siber yang dimaksud.
3. Penelitian ini tidak akan memasukkan analisis terhadap jenis serangan siber lainnya selain brute force attack, dan juga tidak akan membahas implementasi tindakan pencegahan terhadap serangan yang terdeteksi.
4. Variable-variable yang akan di analisis terutama mencakup pola-pola serangan brute force attack yang dapat diidentifikasi melalui data log honeypot cowrie, seperti alamat IP Address Penyerang, alamat IP Address Korban, dan pola percobaan login yang mencurigakan.
5. Evaluasi keberhasilan algoritma Naïve Bayes akan difokuskan pada tingkat Akurasi, Presisi, Recall, dan F1-Score dalam membedakan serangan siber brute force attack dari traffic normal.

Dengan mengindentifikasi batasan-batasan ini, penelitian dapat difokuskan pada analisis serangan brute force attack dengan menggunakan pendekatan yang terstruktur dan terfokus, sesuai dengan lingkungan virtual PT. Riwtech Workshop Indonesia.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menyelidiki terkait efektivitas algoritma Naïve Bayes dalam mendeteksi serangan siber Brute Force Attack berdasarkan data log dari Honeypot Cowrie di lingkungan virtual PT. Riwtech Workshop Indonesia. tujuan spesifik dari penelitian ini adalah sebagai berikut :

1. Untuk mengidentifikasi pola serangan siber Brute Force Attack yang dapat diidentifikasi melalui analisis data log dari Honeypot Cowrie
2. Untuk mengukur tingkat keberhasilan algoritma Naïve Bayes dalam membedakan serangan brute force attack dari traffic normal berdasarkan data log Honeypot Cowrie
3. Untuk mengevaluasi kinerja algoritma Naïve Bayes menggunakan beberapa metrik evaluasi, yaitu Akurasi, Presisi, Recall dan juga F1-Score
4. Untuk menyajikan informasi yang dapat membantu dalam meningkatkan keamanan internal server di PT. Riwtech Workshop Indonesia melalui sebuah lingkungan virtual yang akan dibangun menyerupai lingkungan aslinya.

1.5 Manfaat Penelitian

Ada beberapa manfaat yang ingin dicapai melalui peneltian ini, yaitu :

1. **Meningkatkan Keamanan Internal Server:** Dengan memahami pola serangan siber brute force attack yang umum terjadi dan menggunakan algoritma naïve bayes untuk mendeteksi serangan tersebut, PT Riwtech Workshop Indonesia dapat meningkatkan keamanan jaringan internal server

mereka dengan mengambil tindakan pencegahan yang sesuai dengan jenis serangan yang dimaksud.

2. **Deteksi Dini Serangan Siber:** Penelitian ini akan membantu dalam mendeteksi serangan brute force attack lebih awal dikarenakan kita akan menggunakan media Honeypot Cowrie sebagai umpan kepada penyerang, sehingga diharapkan tidak ada kerugian yang signifikan akibat suatu *event attack* yang terjadi pada internal server. Dan juga diharapkan para stakeholder dari perusahaan terkait bisa mengambil tindakan responsive untuk mengurangi dampak serangan tersebut pada infrastruktur IT pada perusahaan terkait.
3. **Peningkatan Efisiensi Operasional:** Dengan menggunakan algoritma Naïve Bayes untuk otomatisasi deteksi serangan Brute Force Attack, PT Riwtech Workshop Indonesia diharapkan dapat meningkatkan efisiensi operasional dan mengurangi waktu respons terhadap serangan.

Dengan ini, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam upaya meningkatkan keamanan informasi dan infrastruktur jaringan server di PT Riwtech Workshop Indonesia serta menyumbangkan pengetahuan baru dalam bidang deteksi serangan siber.

1.6 Metode Penelitian

1.6.1 Metode Pengumpulan Data

Penelitian ini menggunakan data log yang dihasilkan oleh *Honeypot Cowrie* sebagai sumber data utama. *Honeypot Cowrie* merupakan sebuah honeypot yang dirancang untuk menarik serangan siber *Brute Force Attack* terhadap layanan *SSH* palsu. Dalam lingkungan virtual , *Honeypot Cowrie* bertindak sebagai umpan | target palsu yang menarik serangan siber sehingga dapat merekam perilaku penyerang.

1.6.2 Metode Pengembangan Sistem

Metodelogi yang digunakan dalam pengembangan Model *Naïve Bayes* untuk menganalisa Data Log dari *Honeypot Cowrie* ini akan menggunakan salah satu kerangka kerja *data mining*, yaitu CRISP-DM (*Cross-Industry Standard Process for Data Mining*). CRISP-DM memiliki beberapa tahapan, yaitu :

a. **Business Understanding**

   Pada tahapan ini akan berfokus untuk memahami tujuan bisnis dari proyek yang akan dikerjakan. Ini akan melibatkan beberapa *stakeholder* atau *enduser* dalam mengidentifikasikan sebauh permasalahan dan peluang yang bisa dimanfaatkan.

b. **Data Understanding**

Pada tahap ini, akan dilakukan pengumpulan data, mengevaluasi jumlah dan nilai, serta memahami karakteristik dari struktur data yang akan di analisa.

c. **Data Preparation**

Pada tahapan ini, akan disiapkan kumpulan data yang sudah didapatkan dari proses sebelumnya, untuk dianalisa lebih lanjut. Pada proses ini akan mencakup beberapa proses seperti pembersihan data, penggabungan data, pemilihan atribut yang relevan, serta beberapa proses lainnya yang relevan dengan proses terkait.

d. Modeling

Di tahap ini, akan dibangun sebuah model AI menggunakan algoritma *Naïve Bayes* . Proses ini akan melibatkan data yang sudah diproses pada tahapan CRISP-DM sebelumnya.

e. **Evaluation**

Tahapan evaluasi akan digunakan untuk mengevaluasi model yang sudah dibangun pada proses sebelumnya. Akan dilakukan beberapa skema pengujian model terkait akurasi , presisi, recall, serta F1-Score atau bisa disebut *Confussion Matrix*.

f. Deployment

Setelah model AI yang dibangun sudah memenuhi *goal* dari proyek yang sedang dikerjakan, akan dilakukan tahapan deployment model AI pada platform yang relevan seperti *Cloud Native,* atau media lainnya yang relevan dengan topik akhir.

1.7 Sistematika Penulisan Skripsi

Penyusunan laporan penelitian akan disusun dalam format seperti point-point berikut ini :

BAB I PENDAHULUAN

Pada bab pertama ini, penulis akan menguraikan point-point seperti latar belakang, rumusan masalah, batasan-batasan masalah , tujuan dan manfaat, lokasi penelitian dan pengguna sistem, teknik pengumpulan data, metoda yang digunakan dalam pengembangan sistem, serta sistematika penulisan skripsi itu sendiri.

BAB II LANDASAN TEORI

Pada bab selanjutnya, yaitu bab II, penulis akan mencoba menguraikan perbadingan penelitian terdahulu yang penulis jadikan acuan dengan penelitian saat ini, serta landasan teori yang terkait mengenai konsep-konsep dasar pada penlitian yang dilakukan penulis dan menguraikan komponen-komponen serta factor-faktor pendukung lainnya dalam rancangan sistem.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab III, penulis akan menjelaskan bagaimana sistem dibangun dan diimplementasikan kedalam sebuah lingkungan terkait. Bab ini bersisi detail dari keseluruhan perangkat teknologi yang penulis angkat, seperti metoda algoritama, jenis honeypot, traffic enginnering, dan beberapa hal teknis lainnya.

BAB IV IMPLEMENTASI HASIL

Pada bab IV, bab ini merupakan implementasi hasil, dimana penulis akan menguraikan pembahasan terkait hasil dari rancangan sistem yang sudah dibangun oleh penulis, tampilan interface, hasil confussion matrix, dan beberapa hasil eveluasi yang mungkin nanti bisa bisa dimanfaatkan oleh beberapa stakeholder dari organisasi terkait.

BAB V KESIMPULAN DAN SARAN

Bab V merupakan bab terakhir, dimana penulis akan menguraikan beberapa point kesimpulan dari setiap pembahasan dari setiap bab-bab sebelumnya yang penulis sudah paparkan sebelumnya, serta penulis juga memberikan saran yang diharapkan dapat berguna bagi penelitian berikutnya di masa yang akan mendatang mengingat teknologi dan keamanan sistem akan terus berkembang menyesuaikan kebutuhan industri.