BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan terbaru dalam teknologi jaringan telah membuka peluang yang sangat luar biasa untuk kerentanan system dalam sistem yang digunakan di seluruh dunia. Sebuah perusahaan atau individu akan berjuang dengan mengamankan beberapa hal penting, data berharga, data rahasia, dan data pribadi. Jika melihat secara mendalam infrastruktur perusahaan dalam perusahaan bisnis modern, teknologi informasi muncul sebagai komponen yang paling terlihat [1]. Deteksi ancaman dapat dicapai dengan membuat aturan dasar untuk lalu lintas jaringan tertentu dan menganalisis statistik paket data yang melewatinya. Dalam beberapa kasus dari informasi keamanan *cyber* menjadi pusat perhatian mengingat kerentanan ekosistem komputasi dengan sistem jaringan yang semakin beralih ke tangan peretas. Namun pada kenyataannya, deteksi ancaman hanyalah fungsi dasar yang memerlukan pengetahuan tambahan untuk mengotomatiskan ekstraksi data *firewall* [2].

Firewall adalah perangkat lunak dan perangkat keras sistem yang melindungi jaringan internal dari serangan yang berasal dari luar Internet, dengan memfilter dan mengelola lalu lintas internet [3]. Firewall telah menjadi alat penting dalam mengamankan infrastruktur jaringan. Firewall berada di garis depan dalam melindungi jaringan. Jika aturan firewall tidak dikonfigurasi dengan benar, efektivitas perlindungan firewall akan berkurang. Disisi lain firewall berfungsi untuk melindungan, menyaring, membatasi, dan menolak dari ancaman yang ada. Sehingga semua data yang masuk dapat diidentifikasi untuk difilter, dan aktivitas firewall akan dicatat sebagai *log* yang dapat digunakan sebagai langkah admin untuk meningkatkan keamanan [4]. Untuk menemukan adanya indikasi serangan firewall, pada penelitian terdahulu yang dijadikan referensi sebagai perbandingan dan acuan pada penelitian ini menggunakan berbagai metode.

Proses identifikasi serangan pada jaringan komputer dibagi menjadi dua kategori yaitu deteksi intrusi dan deteksi anomali dari segi informasi yang digunakan pada fase learning. Deteksi intrusi menggunakan lalu lintas normal dan lalu lintas serangan. Metode deteksi anomali mencoba memodelkan perilaku normal sistem, dan peristiwa apa pun yang melanggar model ini dianggap sebagai perilaku yang mencurigakan [5]. Salah satu cara untuk menggunakan model *Machine Learning* sering digunakan untuk mendeteksi intrusi karena pemahaman mereka tentang sistem deteksi intrusi dalam meminimalkan ancaman keamanan. Pemanfaatan dari beberapa algoritma yang ada dalam permodelan *machine learning* seperti *decision tree, firewall* dapat memprediksi aktivitas jaringan normal dan tidak normal. Pemanfaatan algoritma di atas bertujuan untuk salah satu tujuan dari firewall adaptive kemudian dapat memperbarui konfigurasinya untuk memblokir akses tidak sah dan mengizinkan akses resmi [6]. Banyak metode yang digunakan untuk memantau keberadaan malware di komputer, salah satunya menggunakan *Artificial Intelligence* (AI) .

Dalam beberapa tahun terakhir, kecerdasan buatan (AI) menjadi pilihan untuk melakukan analitik di sejumlah bidang, termasuk keamanan siber, salah satunya menggunakan *Machine Learning* [7]. Pada penelitian ini peneliti menggunakan satu algoritma dari supervised learning yaitu *Decision Tree* yang nantinya mendukung dalam mengklasifikasi dan memprediksi adanya serangan *firewall*. Untuk mendukung proses dari klasifikasi dari *Decision Tree* yang dimana penggunaan satu algoritma untuk pemrosesan data membutuhkan waktu yang lama. Salah satu metode yang digunakan dalam pemanfaatan model *machine learning* untuk mengurangi waktu pemrosesan yakni menggunakan wrapper. Wrapper sendiri yaitu berfungsi untuk mencari fitur yang paling cocok pada algoritma yang digunakan dan bertujuan untuk meningkatkan kinerja dari algoritma tersebut [8].

Metode wrapper sendiri berdasarkan pada algoritma pencarian keseluruhan dikarnakan mengevaluasi semua kemungkinan kombinasi fitur dan memilih salah satu yang menghasilkan hasil terbaik [10]. Tujuan dari penelitian ini untuk memprediksi tingkat *accuracy* , aktivitas *legal* dan *ilegal* pada suatu jaringan yang ada pada firewall. Hasil dari penelitian ini yaitu menjadi acuan dalam pemilihan algoritma yang tepat dalam penelitian-penelitian selanjutnya.

1.2 Rumusan Masalah

Penelitian terkait dengan model machine learning untuk proses deteksi web phising secara adaptive sampai dengan saat ini masih banyak dilakukan menggunakan proses klasifikasi tunggal. Oleh karena itu, pada penelitian ini akan melihat bagaimana pengaruh fitur wrapper dalam meningkatkan kinerja dari proses deteksi firewall secara adaptive?

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan-batasan sebagai berikut:

a. Dataset menggunakan CICIDS 2017 (*Intrusion Detection Evaluation Dataset*) dari Kaggle Repository
b. Metode wrapper untuk pemilihan fitur dapat dibagi menjadi tiga kategori: *Forward selection, Backward elimination dan Recursive Feature elimination*
c. Membuat rule dari firewall itu sendiri, dimana pada saat proses pengecekan log aktivitas yang tidak lazim apakah akan di *allow, deny,* dan *drop*

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam pembuatan laporan skripsi ini adalah "Menerapkan teknik fitur wrapper untuk meningkatkan deteksi firewall menggunakan model Machine Learning, dan juga untuk memprediksi tingkat accuracy , aktivitas *legal* dan *ilegal* pada suatu jaringan yang ada pada firewall "

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat untuk peneliti tentang proses deteksi firewall secara adaptive, diantaranya:

a. Penelitian ini diharapkan bisa bermanfaat untuk pengembangan deteksi firewall secara adaptive di masa depan
b. Bagi peneliti, penelitian ini digunakan untuk mengetahui pengaruh fitur wrapper dalam proses konfigurasi deteksi firewall secara adaptive, sehingga menghasilkan kinerja yang lebih baik.

1.6 Sistematika Penulisan

Sistematika penulisan berisikan garis besar atau gambaran secara umum penelitian ini sehingga mempermudah alur isi. Adapun garis besar isi skripsi ini adalah sebagai berikut :

Bab I Pendahuluan, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang, masalah penelitian, dan sistematika penyajian.

Bab II Landasan Teori, pada tahap ini menjelaskan tentang tinjauan kepustakaan dari penelitian-penelitian sebelumnya terkait pembahasan beberapa teori antara lain *firewall, machine learning(ml) Wrapper , Decision Tree(dt)*, dataset *CICIDS-2017*, dan tool yang digunakan pada saat proses pembuatan modeling dan testing.

Bab III Metode Penelitian, bab ini berisi tentang gambaran umum dari alur penelitian, prosedur, dan mekanisme dari metode analisis yang diterapkan pada penelitian.

Bab IV Hasil Dan Pembahasan, bab ini membahas tentang bagaimana cara menampilkan hasil dari modeling, training, dan implementasi analisis dari yang ditemukan pada metode. Dan juga menyampaikan pembahasan secara teknis dari hasil Analisa yang sudah dilakukan.

Bab V Penutup, bab ini menjelaskan tentang tahapan akhir dari peneliti dan memuat kesimpulan dari keseluruhan proses bab-bab sebelumnya. Pada tahapan ini juga menjelaskan tentang kekurangan serta saran untuk pengembangan penelitian berikutnya.