BAB I PENDAHULUAN

1.1 Latar Belakang

Pada era digital seperti sekarang ini, jaringan komputer digunakan sebagai hal untuk menunjang segala kebutuhan manusia. Namun, disisi lain keamanan jaringan komputer juga dinilai rentan akan serangan yang dilakukan pelaku kejahatan untuk memanfaatkan informasi penting yang berhasil dicuri.

Pada penelitian ini digunakan algoritma hidden markov model untuk mendeteksi adanya jenis serangan DoS dan Heartbleed berdasarkan dari dataset yang digunakan. DoS merupakan jenis serangan yang dapat membanjiri jaringan dengan jumlah *traffic* anonim yang besar sehingga dapat menyebabkan sebuah situs menjadi tidak dapat diakses [1]. Heartbleed merupakan suatu bug yang dapat mengambil data yang telah di proteksi oleh OpenSSL [2].

Pada dataset yang digunakan untuk penelitian ini kuantitasi vektor dikelompokkan menggunakan K-Means untuk membuat label pengelompokkan setiap data traffic yang masuk sebelum diestimasi ke parameter algortima HMM.

Algoritma HMM merupakan salah satu metode yang digunakan pada mesin *learning* untuk mendeteksi dan memprediksi serangan siber. Pada dasarnya HMM dapat mendeteksi isntrusi yang tidak dapat diketahui, memprediksi potensi langkah lanjutan yang akan dilakukan oleh *intruder,* dan dapat memproses aliran data yang masuk secara *real-time* [3].

1.2 Rumusan Masalah

Dalam pengoptimalisasian penggunaan algoritma HMM untuk mendeteksi serangan DoS dan *Heartbleed* terdapat rumusan masalah yang digunakan dalam penulisan ini adalah sebagai berikut:

1. Bagaimana implementasi algoritma HMM dalam mendeteksi serangan DoS dan *Heartbleed?*
2. Bagaimana hasil akurasi dari penggunaaan algoritma HMM untuk mendeteksi serangan DoS dan *Heartbleed*?

1.3 Topik dan Batasannya

Penelitian dilakukan dengan menggunakan dataset yang telah disediakan oleh Canadian Institude for Cybersecurity. Data yang digunakan tersebut adalah Intrusion Detection Evaluation Dataset (CIC-IDS 2017). Pada dataset ini berisi serangan benign (normal human activities) dan beberapa serangan umum yang up-to-date, sebagaimana data yang biasa digunakan pada kejadian nyata (PCAPs). Dataset CIC-IDS2017 berisi hasil analisis lalu lintas jaringan dari CICFlowMeter dengan arus yang diberi label berdasarkan timestamp, IP source dan IP destination, source dan destination port, protocol, dan jenis serangan dalam file CSV. Periode pengambilan sample dimulai pada hari Senin, 3 Juli 2017 pukul 09.00 dan berakhir pada hari Jum'at, 7 Juli 2017 pukul 17.00 dengan durasi pengambilan sample selama 5 hari. Pada sejumlah serangan yang telah ditemukan saat pengambilan data, dari dataset tersebut fokus utama dari penelitian ini ialah sample data penelitian di hari Rabu, 5 Julli 2017. Pada hasil sample yang didapatkan pada hari rabu ditemukan 6 jenis serangan yang terdeteksi oleh sistem yaitu: Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowris, dan Heartbleed. Berdasarkan dari hasil tersebut, sample data pada hari rabu memiliki jenis serangan paling banyak dibandingkan dengan sample data pada hari lain [4]. Pada penelitian ini diambil sample data dari masing-masing jenis serangan yang terdapat pada data di hari Rabu, 5 Juli 2017 sebanyak 2511 data.

1.4 Tujuan

Tujuan dari penelitian ini adalah dapat mengimplementasikan algoritma HMM untuk mendeteksi serangan DoS dan *Heartbleed* dengan menggunakan K-Means untuk mengelompokkan setiap data

serangan pada dataset dan menggunakan *confusion matrix* untuk mengukur performa dari penggunaan algortima HMM, serta dapat melakukan analisis berdasarakan hasil pengujian yang didapat.

1.5 Organisasi Tulisan

Pada penulisan penelitian ini, secara garis besar setiap babnya disusun sebagai berikut:

1. Pendahuluan yang berisi tentang latar belakang, topik dan batasan dari penelitian, tujuan dari penelitian, dan organisai penulisan.
2. Studi terkait mengenai penelitian.
3. Sistem yang digunakan untuk penelitian.
4. Evaluasi hasil pengujian dan analisis dari hasil pengujian.
5. Kesimpulan dan saran dari hasil penelitian.
6. Daftar pustaka sebagai acuan dalam melakukan penelitian.