BAB I

PENDAHULUAN

1.1 Latar Belakang

Distributed Denial-of-Service (DDoS) adalah sebuah serangan jaringan yang sangat sering terjadi dalam lingkup jaringan Internet, dimana intensitas dan volume DDoS terus meningkat setiap tahunnya (Hoque *et al,* 2015). Pada saat ini, serangan DDoS masih termasuk salah satu ancaman utama dunia Internet dan menjadi sumber utama pada masalah keamanan *cyber-world* (Networks, 2016). DDoS merupakan suatu ancaman permanen bagi *user*, organisasi, maupun infrastruktur yang ada dalam jaringan Internet. Disisi lain, serangan DDoS sangat berkontribusi atas timbulnya resiko baik dari segi kerahasiaan, integritas, serta ketersediaan *resource* yang disediakan dan dimiliki oleh sebuah organisasi pada jaringan Internet [1].

Klasifikasi paket jaringan yang melewati *router* pada suatu organisasi yang tekoneksi dengan jaringan Internet merupakan sebuah proses yang fundamental dan mutlak untuk dilaksanakan dalam rangka meminimalisir adanya resiko serangan DDoS [2]. Pada umumnya, proses deteksi dini terhadap serangan DDoS dilaksanakan oleh *Intrusion Detection System* (IDS) yang terpasang pada sistem router organisasi, namun teknik deteksi yang dilaksanakan oleh IDS dapat dikatakan jauh dari sempurna apabila dibandingkan dengan semakin bervariasinya teknik dan metode serangan *cyber* yang semakin modern [1]. Secara teknis, *Intrusion Detection System* bekerja dengan cara memonitor dan memberikan *flag* terhadap aktivitas mencurigakan yang terjadi dalam jaringan dan langsung di-

report sebagai *alert*, sehingga menimbulkan dampak terhadap tingginya rata-rata deteksi yang bersifat *false-positive* serta ukuran volume *alert* yang terus membesar, karena *traffic* data yang ada dalam jaringan merupakan suatu hal yang bersifat *non-stationary* [3].

Sering terjadinya serangan DDoS membuat adanya ancaman terhadap pengguna internet atau *server*, maka dari itu diperlukannya pengenalan baru beberapa metode untuk mendeteksi serangan DDoS yang terjadi, diantaranya dapat menggunakan metode IDS (*Intrusion Detection System*) yang sebelumnya sudah ada lebih dulu untuk mendeteksi serangan DDoS. Pada umumnya serangan DDoS terbagi menjadi 3 jenis yaitu serangan dengan basis *bandwith*, serangan dengan lalu lintas jaringan dan serangan dengan basis aplikasi (Geges dan Wibisono, 2015). Metode Neural Network secara algoritma EM (*Expectation-Maximization*) digunakan untuk mendeteksi adanya serangan DDoS. Menurut dataset DARPA ada 21 kelompok serangan yang dapat dikelompokkan menjadi 13 kelompok serangan, sehingga terjadi kesalahan pemisahan *alert* dari jenis serangan yang sama, sehingga menjadi serangan yang berbeda [4].

Selanjutnya dalam pendeteksian serangan DDoS dalam internet juga dapat dilakukan dengan metode *live forensik*. *Digital forensiks* berkaitan dengan lalu lintas internet, internet sebagai media untuk mendapatkan dan sekaligus untuk pertukaran informasi sangat rentan dengan penyalahgunaan informasi. Era *big data* saat ini membuat data informasi sangatlah rentan dengan kejahatan termasuk pada jaringan internet dalam organisasi. *Digital forensiks* sebagai suatu ilmu untuk menemukan barang bukti dari kejahatan yang telah terjadi yang *valid* atau dapat dipertanggungjawabkan di pengadilan. *Digital forensiks* ini dibagi menjadi dua

teknik yaitu *live forensiks* dan *dead forensiks*. Teknik *live forensiks* ini sangat bergantung pada keadaan komputer yang sedang menyala, karena membutuhkan data yang berjalan pada *Random Access Memory* (RAM). Data pada RAM disebut juga *data volatile* atau data sementara yaitu data yang hanya terdapat saat komputer menyala jika komputer mati maka data itu akan hilang. Digital forensiks pada intinya adalah menemukan bukti digital bisa tersimpan pada penyimpanan komputer sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan, dan lainnya. *Digital forensik* kemudian berkembang menjadi sesuatu yang penting dalam keamanan informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan dipecahkan/diselesaikan pada penelitian ini, yang menjadi permasalahan ini adalah apakah terdapat perbedaan hasil deteksi serangan DDoS dengan menggunakan metode *live forensik* dan metode *neural network* yang didasarkan pada statistik log jaringan dalam mendeteksi serangan DDoS pada paket jaringan yang melewati *router*.

1.3 Batasan Masalah

Untuk memfokuskan penelitian ini, maka penelitian memberikan pembatasan masalah penelitian yaitu :

1. Penelitian ini hanya difokuskan pada serangan *Distributed Denial of Service* (DDoS) saja, tidak untuk jenis serangan lain.

2. Sistem jaringan komputer berbasis Sistem operasi
3. Penelitian di lakukan menggunakan perangkat *Router*
4. Untuk menemukan dan mengumpulkan bukti *digital* menggunakan fasilitas *log* pada sistem operasi *router*
5. Metode yang digunakan meliputi metode *live forensik* dan metode *neural network.*
6. Penelitian ini dibuat secara kepustakaan (*library research*).

1.4 Maksud dan Tujuan Penelitian

Penelitian ini memiliki tujuan untuk membandingkan hasil deteksi serangan DDoS dengan menggunakan metode *live forensik* dan metode *neural network* yang didasarkan pada statistik log jaringan dalam mendeteksi serangan DDoS pada paket jaringan yang melewati *router*.

1.5 Manfaat Penelitian

Pentingnya nilai manfaat untuk kemajuan dalam bidang teknologi informasi yang memberikan nilai tersendiri sehingga dapat digunakan sebaik mungkin. Adapun manfaat penelitian adalah sebagai berikut:

1. Dapat mengetahui dan mencegah terjadinya gangguan jaringan internet dalam organisasi akibat adanya serangan DDoS.
2. Diharapkan dapat meningkatkan akses kerja jaringan komputer dan dampaknya kinerja organisasi juga makin membaik.

1.6 Sistematika Penulisan

Sistematika yang digunakan dalam penyusunan skripsi ini adalah:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, dan sistematika penulisan

Bab II LANDASAN TEORI.

Bab ini menguraikan tentang pengertian forensik, komputer forensik, prinsip, kebijakan dan prosedur komputer forensic, perangkat komputer forensik, permodelan forensik, forensik jaringan, *neural network,* metode live forensik, dan *router.*

Bab III METODE PENELITIAN

Dalam bab ini akan diuraikan tentang alur penelitian ini dilakukan

Bab IV ANALISIS DAN PEMBAHASAN

Bab ini berisi tentang uraian-uraian metode *live forensik* dan metode *neural network* yang didasarkan pada statistik log jaringan dalam mendeteksi serangan ddos pada paket jaringan yang melewati *router*

Bab V PENUTUP

Bab ini berisi kesimpulan hasil analisis dan memberikan masukan atau saran bagi perbaikan penelitian kedepannya.