

BAB I

PENDAHULUAN

A. Latar Belakang

Menjaga validitas dan integritas data menjadi hal yang sangat penting (Arta et al., 2018). Salah satu caranya adalah dengan keamanan jaringan. Bukan hanya untuk menjaga validitas dan integritas data, keamanan jaringan juga memungkinkan layanan kepada pengguna (Arta et al., 2018). *Server* jaringan komputer dapat diserang kapan saja, ketika administrator sedang beroperasi atau tidak. Oleh karena itu, dibutuhkan sistem keamanan yang mampu mendeteksi dan menanggulangi secara langsung ancaman-ancaman terhadap infrastruktur jaringan.

Menurut Sharafaldin dalam Santoso et al. (2022), serangan jaringan komputer yang kuat meskipun bisa dibilang relatif sederhana dalam menyerang sumber daya dari target adalah *Distributed Denial of Service* (DDoS). Salah satu akibatnya adalah pengguna yang legal tidak dapat mengakses layanan. *Distributed Denial of Service* (DDoS) dapat dikatakan serangan yang terstruktur, cara kerjanya adalah mencoba menyerang dengan sejumlah sistem komputer dan menjadikan komputer *server* sebagai target agar jumlah lalu lintas menjadi tinggi hingga *server* menjadi tidak dapat menangani permintaannya (Santoso et al., 2022).

Sistem yang dapat otomatis mendeteksi tindakan mencurigakan yang kemungkinan membahayakan dalam jaringan adalah *Intrusion Prevention System* (IPS). Alur kerja dari IPS adalah meninjau paket yang berasal dari luar jaringan, lalu mengidentifikasi paket apakah aman atau tidak menggunakan file konfigurasi yang berisi *rules*. Jika tidak aman, maka IPS akan memberikan

peringatan kepada administrator dan akan menghapus dari jaringan. Selain itu, IPS juga mampu memblokir akses pada lalu lintas jaringan dengan menggunakan fitur *Intrusion Detection System (IDS)* dan *firewall*.

Salah satu perangkat lunak deteksi intrusi dan pencegahan intrusi yang bersifat *open source* adalah *Suricata*. Kemampuan yang dimiliki oleh *Suricata* adalah mampu mengidentifikasi atau mendeteksi dan mencegah sebuah ancaman serangan terhadap sistem dengan menggunakan *rules* yang terintegrasi. Alur kerja dari *Suricata* adalah pertama ketika terjadinya penyerangan, maka *Suricata* akan mengecek paket/serangan yang masuk melalui *rules* yang sudah dibuat. *Suricata* akan membuat log serangan ketika mendeteksi paket yang datang tersebut adalah serangan.

SMA Muhammadiyah 5 Karanggeneng yang berada di Kabupaten Lamongan, merupakan institusi yang bergerak di bidang pendidikan. Salah satu fasilitas pendukung pembelajaran dalam SMA Muhammadiyah 5 Karanggeneng adalah terdapatnya laboratorium yang juga menyediakan jaringan internet. Berdasarkan observasi dan wawancara yang dilakukan dengan Bapak Zainul Rokhim, S.Pd. selaku guru yang sering menangani masalah jaringan komputer sekolah, menyatakan bahwa di SMA Muhammadiyah 5 Karanggeneng kurangnya keamanan jaringan yang diterapkan. Beliau memaparkan bahwa keamanan jaringan yang ada hanya berasal dari *server* pusat atau bawaan dari Access Point, sehingga administrator tidak dapat mendeteksi adanya serangan ketika jaringan bermasalah. Beliau juga memaparkan bahwa jaringan yang ada kadang mengalami penurunan

performa biasanya lebih dari 5 kali setahun sehingga proses pembelajaran kadang terganggu.

Dari hasil observasi, SMA Muhammadiyah 5 Karanggeneng yang memiliki puluhan PC yang terhubung ke dalam *network* dan memiliki koneksi internet dengan kurang adanya keamanan atau pendeteksian lalu lintas data serta paket yang masuk, dapat berpotensi diserang oleh pihak yang tidak bertanggung jawab sehingga mengakibatkan penurunan performa jaringan maupun komputer. Hal ini dapat mengganggu jalannya proses pembelajaran dan aktivitas yang berjalan menggunakan jaringan internet.

Penelitian terdahulu yang relevan yakni penelitian yang dilakukan oleh Firdaus & Suartana (2021), yang bertujuan untuk mengimplementasikan *Suricata* untuk *Intrusion Detection/Prevention System* menggunakan PFsense. Hasil penelitian yang didapatkan adalah fitur *Suricata IDPS* pada Sistem Operasi PFsense dapat mendeteksi serangan dan dapat memblokir (drop) terhadap serangan tersebut dengan menggunakan *rules* yang telah dibuat.

Penelitian yang dilakukan Adesty et al. (2020), meneliti dan menerapkan *Intrusion Prevention System (IPS) Suricata* sebagai keamanan terhadap *Distributed Denial of Service (DDoS) attack*. Hasil penelitian yang didapat adalah bahwa IPS berbasis *Suricata* dapat melakukan deteksi ketika adanya serangan DDoS dan dapat melakukan blokir akses terhadap serangan tersebut dengan menggunakan fitur *firewall* yaitu *IPTables*.

Penelitian yang relevan selanjutnya dilakukan oleh Santoso et al. (2022), yang melakukan penelitian dengan tujuan untuk mengimplementasikan dan menganalisa snort dan *Suricata* sebagai *Intrusion Detection System* dan

Intrusion Prevention System untuk mencegah serangan DoS dan DDoS. Penelitian ini menggunakan pengujian keamanan jaringan yang diterapkan dengan beberapa skenario penyerangan yaitu *Syn Flood*, *Ping of Death* dan HTTP Flood. Persamaan dari penelitian ini yakni penggunaan Suricata sebagai keamanan jaringan dan Iptables sebagai *firewall*.

Dari hasil observasi, wawancara, dan penelitian relevan tersebut maka peneliti mengembangkan keamanan jaringan menggunakan *Intrusion Prevention System* berbasis *Suricata* dalam mendeteksi dan mencegah *Distributed Denial of Service* (DDoS) di SMA Muhammadiyah 5 Karanggeneng. Berdasarkan penelitian yang dilakukan Santoso et al. (2022) yang menggunakan 3 macam serangan, peneliti mengutip beberapa serangan yang akan diuji cobakan pada penelitian ini yakni serangan *Syn Flood* dan *Ping of Death*. *Suricata* akan dibangun dalam sistem operasi ubuntu. Dan peneliti pun tertarik untuk melakukan penelitian dengan judul “Pengembangan Keamanan Jaringan Menggunakan *Intrusion Prevention System* Berbasis *Suricata* Terhadap *Distributed Denial Of Service*”.

B. Rumusan Masalah

Berdasarkan terhadap latar belakang yang sudah diuraikan, peneliti menentukan rumusan masalah seperti berikut :

1. Bagaimana pengembangan *Intrusion Prevention System* berbasis *Suricata* sebagai keamanan jaringan terhadap *Distributed Denial of Service* di SMA Muhammadiyah 5 Karanggeneng?
2. Bagaimana hasil pengujian *Intrusion Prevention System* berbasis *Suricata* sebagai keamanan jaringan terhadap *Distributed Denial of Service*?

C. Tujuan Penelitian Pengembangan

1. Untuk mengembangkan *Intrusion Prevention System* berbasis *Suricata* sebagai keamanan jaringan terhadap *Distributed Denial of Service* di SMA Muhammadiyah 5 Karanggeneng
2. Untuk mengetahui hasil pengujian *Intrusion Prevention System* berbasis *Suricata* sebagai keamanan jaringan terhadap *Distributed Denial of Service*

D. Spesifikasi Produk yang Diharapkan

Spesifikasi produk yang diharapkan peneliti dalam penelitian ini adalah sebagai berikut :

1. *Suricata* adalah *software* yang bersifat sumber terbuka, dapat digunakan untuk mendeteksi dan mencegah ancaman pada jaringan komputer.
2. *Ubuntu* adalah Sistem Operasi yang digunakan untuk menginstall *Suricata*
3. Komputer *server* adalah sebuah perangkat keras yang akan digunakan sebagai tempat untuk konfigurasi *Suricata*
4. *Tools Hping3* adalah sebuah alat yang akan peneliti gunakan untuk menguji keamanan pada jaringan tersebut.
5. *Software Virtual Box* adalah sebuah alat untuk membuat virtualisasi didalam sebuah komputer, disini peneliti akan gunakan untuk diisikan operasi sistem *ubuntu* sebagai tempat penginstallan *Suricata* dan *tools Hping3*

E. Batasan Penelitian Pengembangan

Terdapat beberapa batasan masalah pada skripsi ini, yaitu :

1. Pengembangan dan penerapan dilakukan pada laboratorium komputer SMA Muhammadiyah 5 Karanggeneng

2. Pengimplementasian menggunakan sistem operasi ubuntu dan perangkat lunak *Suricata*, dan *tools* tambahan *Iptables* sebagai *firewall*
3. Layanan yang digunakan untuk penyerangan adalah *Hping3*
4. Pengujian serangan dilakukan dalam beberapa skenario yaitu *Syn Flood* dan *Ping of Death*.

F. Pentingnya Penelitian Pengembangan

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Manfaat Teoritis
Sistem keamanan yang diteliti efektif sehingga menjadi pendukung untuk penelitian selanjutnya.
2. Manfaat Praktis
 - a. Bagi peneliti, pengembangan keamanan jaringan menggunakan IPS berbasis *Suricata* sebagai keamanan jaringan terhadap DDoS dapat meningkatkan pengetahuan peneliti dalam menangani masalah keamanan yang sering terjadi dalam infrastruktur jaringan
 - b. Bagi sekolah, pengembangan keamanan jaringan dapat membantu administrator dalam mendeteksi dan mencegah serangan yang masuk sehingga jaringan tidak mudah *down* dan kegiatan belajar mengajar tidak terhambat.

G. Definisi Istilah

1. *Intrusion Prevention System* (IPS) adalah sistem yang dengan otomatis melakukan deteksi tindakan mencurigakan yang kemungkinan membahayakan dalam jaringan dan dapat memblokir akses pada lalu lintas

jaringan dengan menggunakan fitur *Intrusion Detection System* (IDS) dan *firewall*.

2. Suricata adalah *software* deteksi intrusi dan pencegahan intrusi yang bersifat sumber terbuka yang mampu mendeteksi dan mencegah sebuah ancaman serangan terhadap sistem dibantu dengan *rules* yang terintegrasi.
3. Keamanan jaringan adalah sistem pertahanan terhadap jaringan dan aplikasi-aplikasinya terhadap serangan atau aktivitas yang berpotensi membahayakan keabsahan dan integritas data.
4. *Distributed Denial of Service* (DDoS) merupakan salah satu percobaan serangan dari sejumlah sistem komputer yang menjadikan sebuah *server* target dengan tujuan agar lalu lintas jaringan menjadi terlalu tinggi hingga *server* tidak dapat menangani permintaanya.