BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, keamanan jaringan telah menjadi salah satu prioritas utama bagi organisasi dan perusahaan di berbagai sektor. Dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi, serangan terhadap infrastruktur jaringan juga semakin canggih dan sering terjadi. Ancaman-ancaman ini tidak hanya berasal dari luar, tetapi juga dapat timbul dari dalam jaringan itu sendiri. Oleh karena itu, perlunya sistem yang mampu mendeteksi dan merespons ancaman secara cepat dan efektif menjadi sangat krusial.

Sistem deteksi intrusi (IDS) memantau peristiwa yang terjadi pada sistem komputer atau jaringan dan menganalisisnya untuk mengidentifikasi kegiatan, termasuk normal atau intrusi. Sistem deteksi intrusi (IDS) dibagi menjadi dua bentuk yang paling umum digunakan dan masing-masing memiliki karakteristik yang berbeda. Yang pertama adalah pengambilan data dari berbagai tingkat sistem, seperti jaringan, host, dan aplikasi. Sistem deteksi intrusi (IDS) adalah kemampuan perangkat keras atau perangkat lunak yang dapat mendeteksi aktivitas mencurigakan pada jaringan dan menganalisis dan mencari. Keduanya harus dikembangkan agar hasilnya lebih baik dalam menemukan setiap infiltrasi dan membuat rencana terbaik [1].

Suricata adalah perangkat lunak berbasis IDS/IPS yang merupakan generasi berikutnya dari perangkat-perangkat IDS/IPS yang ada saat ini. Suricata adalah aplikasi berbasis IDS/IPS yang melakukan deteksi terhadap serangan atau gangguan dengan menggunakan protokol open *source*. metode berbasis tanda tangan yang mengeluarkan peringatan apabila terdapat paket yang dianggap sebagai jenis serangan sesuai dengan peraturan yang dimiliki oleh Suricata. Selanjutnya, administrator akan melacak paket serangan untuk menghentikannya [2], [3].

Implementasi Suricata pada server jaringan bertujuan untuk meningkatkan kemampuan deteksi dan respons terhadap ancaman keamanan. Dengan kemampuan analitik yang kuat, Suricata dapat memberikan wawasan yang mendalam tentang aktivitas jaringan, membantu mengidentifikasi pola serangan, dan memberikan rekomendasi untuk mitigasi ancaman. Ini sangat penting untuk memastikan bahwa

data dan aset organisasi tetap aman dari berbagai jenis serangan. Cara Suricata bekerja adalah dengan mengecek paket atau serangan yang ada melalui aturan yang dibuat ketika adanya penyerangan. Suricata dapat melakukan deteksi otomatis pada *layer* 7, termasuk aplikasi seperti dns, http, imap, ftp, dan smtp, dan akan membuat log serangan ketika serangan terdeteksi. Dengan demikian, Suricata dapat memberikan solusi untuk meningkatkan keamanan komputasi *cloud* berbasis Linux Debian. Berdasarkan informasi ini, penulis telah menerapkan sistem deteksi *intrusion* (IDS) dengan Suricata pada *server virtual private cloud* (VPS) berbasis Linux Debian 9 [4].

Berdasarkan permasalahan diatas maka penulis mengambil judul laporan Kerja Praktikan Lapangan mengenai "**Implementasi Sistem Deteksi Anomali Dan Serangan Jaringan Dengan Metode *Intrusion Detection System* (IDS) Suricata Pada Server"**

1.2 Tujuan

1) Tujuan Pelaksanaan PKL/KP

   Tujusn pelaksanaan PKL/KP sebagai berikut:

   a. Memberikan kesempatan untuk menerapkan pengetahuan dan keterampilan yang diperoleh selama perkuliahan ke dalam praktik kerja di industri atau organisasi.
   b. Memfasilitasi dalam memperoleh pengalaman kerja nyata, memahami dinamika lingkungan kerja, dan mengembangkan kemampuan problem-solving.
   c. Memperkuat ikatan dan kerja sama antara institusi akademik dengan industri atau organisasi mitra.

2) Tujuan Pembuatan Laporan

   Tujuan pembuatan laporan adalah:

   a. Mendokumentasikan proses perancangan, konfigurasi, dan implementasi sistem deteksi anomali dan serangan jaringan menggunakan metode *Intrusion Detection System* (IDS) Suricata pada server.

b. Menganalisis dan mengevaluasi efektivitas penerapan IDS Suricata dalam mendeteksi serta merespons terhadap aktivitas mencurigakan atau serangan pada jaringan komputer
c. Mengidentifikasi keunggulan, keterbatasan, dan tantangan dalam mengimplementasikan IDS Suricata pada infrastruktur server.

1.3 Ruang Lingkup

Ruang lingkup penelitian ini mencakup beberapa aspek utama dalam implementasi dan optimalisasi Suricata sebagai sistem deteksi intrusi (IDS) pada server jaringan. Pertama, penelitian ini akan mengkaji proses instalasi dan konfigurasi Suricata, memastikan integrasinya dengan infrastruktur jaringan yang ada di Dinkominfo. Kedua, fokus pada deteksi anomali dan berbagai jenis serangan jaringan, seperti serangan DoS, DDoS, *brute force*, dan eksploitasi kerentanan. Optimalisasi kinerja Suricata juga akan dilakukan dengan menyesuaikan konfigurasi untuk meningkatkan akurasi dan efisiensi deteksi, serta pemantauan dan pembaruan berkelanjutan agar IDS tetap efektif menghadapi ancaman terbaru. Selain itu, penelitian ini mencakup pengujian dalam lingkungan jaringan yang dikontrol untuk mengevaluasi efektivitas Suricata, menggunakan berbagai skenario serangan untuk menguji respon IDS. Analisis hasil pengujian akan dilakukan untuk menilai keberhasilan implementasi dan optimalisasi. Terakhir, laporan penelitian akan disusun dengan dokumentasi teknis yang lengkap, memberikan panduan praktis dan rekomendasi untuk perbaikan lebih lanjut dalam meningkatkan keamanan jaringan Dinkominfo.

1.4 Aspek Umum Kelembagaan

1) Profil Perusahaan

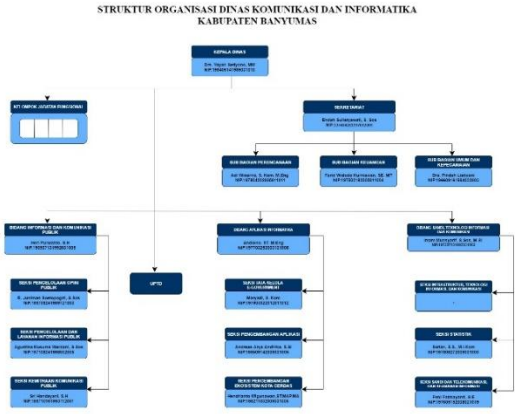
Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas adalah salah satu perangkat daerah yang bertanggung jawab untuk menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika. Menurut Peraturan Bupati Banyumas Nomor 6 Tahun 2016, tujuan dari Dinas Komunikasi dan Informatika Banyumas adalah untuk menjalankan operasi teknis urusan pemerintah daerah bidang komunikasi dan informatika dengan prinsip otonomi dan tugas pembantuan. Dinkominfo Kabupaten Banyumas bertanggung jawab untuk merumuskan,

menetapkan, dan memimpin penyelenggaraan koordinasi kebijakan urusan komunikasi dan informatika, bidang informasi dan komunikasi publik, bidang *e-government*, bidang sandi, dan bidang teknologi informasi dan komunikasi. Fungsi ini diberikan oleh pemerintah daerah dan dibantu oleh kabupaten. Dinkominfo Kabupaten Banyumas bertanggung jawab untuk menyediakan, memberikan, dan atau menerbitkan informasi publik yang berada di bawah kewenangan kepada pihak yang memintanya, termasuk informasi yang dilarang oleh undang-undang. Pasal 7 Undang-Undang Nomor 14 Tahun 2008 menetapkan tanggung jawab badan publik sebagai berikut: (1) memberikan informasi publik yang akurat, benar, dan tidak menyesatkan; (2) membangun dan mengembangkan sistem informasi dan dokumentasi yang efektif untuk mengelola informasi publik sehingga mudah diakses; dan (3) menuliskan pertimbangan politik, ekonomi, sosial, budaya, atau pertahanan dan keamanan negara dalam setiap kebijakan yang dibuat [5].

Dinkominfo Kabupaten Banyumas saat ini bertugas membantu Bupati dalam melaksanakan urusan pemerintahan di bidang komunikasi dan informatika, informasi dan komunikasi publik, *e-government*, sandi, dan teknologi informasi dan komunikasi. Bidang-bidang ini merupakan wewenang dan tugas pembantuan yang diberikan kepada Daerah. Sistem pelayanan informasi dan komunikasi harus beradaptasi dengan tuntutan zaman dan berbasis teknologi informasi saat berkembang. Untuk menggunakan teknologi informasi dengan sukses dalam penyelenggaraan pemerintahan atau *e-government*, hal-hal penting seperti sumber daya manusia, tata kelola, aplikasi, dan data base, serta infrastruktur jaringan. Dinkominfo Kabupaten Banyumas terus berupaya semaksimal mungkin untuk membangun dan meningkatkan pelayanan prima yang berkaitan dengan urusan komunikasi dan informatika kepada masyarakat Kabupaten Banyumas [6].

2) Struktur Organisasi

Berikut ini adalah struktur organisasi dari Dinkominfo kab Banyumas



Gambar 1.4.1 Struktur Organisasi

1.5 Metode Penulisan Laporan

Laporan Kerja Praktik menggunakan metode berikut:

1) Wawancara

Metode ini melibatkan pengumpulan data dan informasi melalui wawancara langsung dengan pihak-pihak terkait, seperti staf Dinkominfo, ahli keamanan jaringan, dan pengguna jaringan. Wawancara bertujuan untuk mendapatkan pemahaman mendalam tentang kebutuhan keamanan jaringan, masalah yang dihadapi, dan pengalaman pengguna terhadap sistem yang ada.

2) Studi Literatur

Studi literatur dilakukan dengan meninjau berbagai sumber pustaka yang relevan, termasuk buku, jurnal, artikel, dan dokumen teknis terkait Suricata dan sistem deteksi intrusi (IDS). Metode ini bertujuan untuk memahami teori-teori dasar, teknik-teknik optimalisasi, dan praktik terbaik dalam implementasi Suricata sebagai IDS. Selain itu, studi literatur juga mencakup peninjauan regulasi dan standar keamanan jaringan yang berlaku.

3) Pengujian Lapangan

Pengujian lapangan melibatkan implementasi dan evaluasi langsung dari Suricata dalam lingkungan jaringan Dinkominfo. Metode ini meliputi instalasi, konfigurasi, dan optimalisasi Suricata, serta pengujian efektivitasnya dalam mendeteksi dan merespons ancaman keamanan. Data

yang diperoleh dari pengujian lapangan akan dianalisis untuk menilai kinerja Suricata dan mengidentifikasi area yang memerlukan perbaikan atau penyesuaian.

1.6 Sistematika Penulisan Laporan

Penulisan Laporan dengan judul ini memiliki beberapa topik pembahasan yang sistematis terdiri dari:

BAB 1 PENDAHULUAN

Bab ini memuat latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup, serta metode penulisan laporan. Pendahuluan memberikan gambaran umum mengenai pentingnya implementasi dan optimalisasi Suricata dalam meningkatkan keamanan jaringan.

BAB 2 DASAR TEORI

Bab ini menjelaskan teori-teori dan konsep-konsep dasar yang relevan dengan sistem deteksi intrusi (IDS), khususnya Suricata. Di dalamnya juga dijelaskan mengenai arsitektur jaringan, ancaman keamanan yang umum terjadi, serta teknik dan strategi optimalisasi Suricata.

BAB 3 HASIL DAN PEMBAHASAN

Bab ini memaparkan hasil dari implementasi dan pengujian Suricata pada infrastruktur jaringan Dinkominfo. Pembahasan mencakup analisis data dari pengujian lapangan, evaluasi kinerja Suricata, serta perbaikan yang dilakukan untuk optimalisasi. Bab ini juga membahas implikasi dari hasil penelitian terhadap keamanan jaringan Dinkominfo.

BAB 4 PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian dan implementasi, serta saran-saran untuk pengembangan lebih lanjut. Kesimpulan menggarisbawahi pencapaian tujuan penelitian dan manfaat yang diperoleh dari penggunaan Suricata. Saran diberikan untuk perbaikan dan peningkatan keamanan jaringan di masa mendatang.

DAFTAR PUSTAKA