BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi memberikan dampak peningkatan pada berbagai bidang dan lingkup penerapannya. Hal ini dapat dilihat dengan mudahnya mendapatkan informasi yang dibutuhkan dari media-media online yang tersebar lewat internet. Bentuk informasi yang dikirim dan diterima lewat internet harus terhubung dengan protokol yang sama agar data yang diterima mudah dibaca dan diolah dengan baik. Jaringan yang terhubung secara luas membuat pengguna merasa dipermudahkan, akan tetapi hal itu tidak selaras jika keamanan jaringan tidak dijaga dengan baik (Sulaksono & Suharyanto, 2020).

Ancaman penyerangan bisa terjadi karena sistem keamanan server dan komputer klien tidak diperkuat dengan baik. Oleh karena itu sistem pertahanan sangat dibutuhkan untuk melindungi data dan menjaga integritas sistem. Universitas Pendidikan Ganesha memiliki *data center* yang terletak pada gedung UPA TIK, yang dimana terdapat sebuah server yang digunakan untuk keperluan *web server* dan *cloud storage*. Terkait sistem keamanan yang diterapkan pada *data center* UPA TIK, terdapat celah keamanan berupa tidak adanya sistem deteksi intrusi pada jaringan, dan rentan terhadap serangan luar maupun serangan dari internal. Jika *data center* UPA TIK tidak terlindungi dengan baik maka dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memaksa masuk dan meretas data yang ada pada server. Sistem deteksi intrusi atau IDS (*Intrusion Detection System*) sangat penting untuk diterapkan di server, selain sebagai

pengawas sistem, IDS juga dapat memberikan peringatan untuk administrator agar segera melakukan tindakan langsung untuk mencegah serangan yang akan terjadi.

Metode yang diterapkan untuk implementasi IDS ini yaitu metode basis *signature rules*, aturan ini dibuat ketika model atau tipe serangan sudah diketahui dan ketika terjadinya serangan yang sama atau memiliki metode serangan yang persis sama, maka sistem IDS akan secara otomatis memberikan peringatan. Proses ini akan dibantu dengan penelitian *action research* yang terdiri dari studi literatur, observasi, wawancara, rancangan topologi jaringan, proses instalasi dan konfigurasi, uji kinerja *rules* IDS serta evaluasi pengujian (Davison et al., 2021). Implementasi IDS yang digunakan adalah sistem deteksi berbasis *signature* dengan tipe NIDS (*Network Intrusion Detection System*) serta menggunakan fitur *port mirroring* pada mikrotik agar IDS suricata bisa memantau lalu lintas jaringan tanpa mengganggu aliran data server. Sistem ini sangat efektif untuk meminimalisir serangan, karena jika paket yang mencurigakan melewati sistem NIDS maka paket tersebut dapat dideteksi serta memberikan output berupa *alarm* peringatan ke administrator.

1.2 Rumusan Masalah

Berdasarkan permasalah yang dijelaskan pada latar belakang diatas, diperlukan evaluasi lebih lanjut terkait implementasi *intrusion detection system* untuk mengatasi potensi serangan pada UPA TIK. Terkait hal ini, penelitian akan memfokuskan pada tiga permasalahan utama, yaitu:

1. Bagaimana cara instalasi dan menjalankan sistem keamanan *intrusion detection system* (IDS) pada *data center* UPA TIK ?.

2. Apakah menggunakan metode NIDS (*Network Intrusion Detection System*) dan *port mirroring* pada proses implementasi IDS dapat melakukan proses pemantaun dan mendeteksi serangan sesuai dengan indikator metrik evaluasi kinerja IDS ?.
3. Bagaimana hasil dari uji coba penggunaan metode deteksi *signature rules* pada sistem keamanan *intrusion detection system* (IDS) untuk mendeteksi serangan ?.

1.3 Tujuan Penelitian

Dari rumusan masalah yang disampaikan mengenai bagaimana cara implementasi dan menguji *intrusion detection system,* adapun tiga tujuan dari penelitian ini yaitu

1. Untuk mengetahui Bagaimana cara implementasi dan menjalankan sistem keamanan *intrusion detection system* (IDS) pada *data center* UPA TIK.
2. Untuk mengetahui apakah menggunakan metode NIDS (*Network Intrusion Detection System*) dan *port mirroring* pada proses implementasi IDS dapat melakukan proses pemantaun dan mendeteksi serangan sesuai dengan indikator metrik evaluasi kinerja IDS.
3. Untuk mengetahui Bagaimana hasil dari uji coba penggunaan metode deteksi *signature rules* pada sistem keamanan *intrusion detection system* (IDS) untuk mendeteksi serangan.

1.4 Manfaat Penelitian

Dengan adanya penilitian tentang sistem keamanan *intrusion detection system* (IDS) diharapkan dapat menambah pengetahuan dan wawasan mengenai

sistem kemanan untuk mengamankan server. Oleh karena itu terdapat dua manfaat yang dapat diperoleh yaitu :

1.4.1 Manfaat Teoritis

Penilitian ini diharapkan dapat membantu meningkatkan pemahaman tentang sistem keamanan jaringan serta memudahkan pengguna untuk melakukan pengembangan terhadap sistem yang ada. selain itu penelitian ini bisa digunakan untuk contoh penerapan sistem dimasa yang akan datang dikarenakan terdapat pola pertahanan yang ada di penelitian ini bisa dimanfaatkan kembali serta dikembangkan dengan teknologi yang lebih baru.

1.4.2 Manfaat Praktis

1. Bagi Mahasiswa

   Penelitian ini dapat dimanfaatkan oleh mahasiswa dalam pengembangan sebagai contoh sistem keamanan, serta pola serangan-seranganya dapat digunakan sebagai acuan untuk menyesuaikan dengan metode pertahanan yang lebih baru. Selain dapat menambah ilmu pengetahuan tentang *intrusion detection system* (IDS) mahasiswa juga bisa memahami bagaimana cara mengamankan sebuah server dari sisi pertahanan jaringan atau dari *host* komputer itu sendiri.

2. Bagi Masyarakat

   Sistem ini bisa digunakan untuk membantu mengamankan jaringan lokal yang memiliki potensi sering diserang oleh orang yang tidak bertanggung jawab. Serta dapat digunakan untuk menambah wawasan terkait pengembangan sistem deteksi untuk mencegah serangan yang dapat

merugikan pengguna. Contohnya mengamankan server pengelolaan data masyarakat suatu daerah atau mengamankan sistem IoT untuk perumahan.

1.5 Batasan Masalah

Dalam pengembangan sistem keamanan ini, peneliti perlu memaparkan batasan masalah terkait implementasi IDS ini agar tidak keluar dari pokok pembasan yang diteliti. Adapun batasan masalah yang dapat dipaparkan sebagai berikut :

1. *Software* yang digunakan untuk implementasi IDS adalah suricata.
2. Metode yang digunakan untuk membuat *rules* atau mendeteksi seranganya adalah metode *signature* dari IDS suricata.
3. Pada implementasi ini tidak membandingkan metode *signature rules* dengan metode deteksi yang lainnya.
4. Website yang di uji coba untuk proses implementasi IDS adalah website versi *development* secara lokal yaitu website sipepeng undiksha (https://sipepeng-ng-dev.undiksha.ac.id/).
5. Proses pengujian akan membandingkan metode *default* dan metode tambahan basis *signature-rules*.
6. Hasil dari penelitian yang harus didapatkan yaitu berhasil mendeteksi serangan menggunakan alat penetrasi ZAP, DOS-Ripper, dan Burpsuite (XSS *Attack*).