BAB 1 PENDAHULUAN

1.1. Latar Belakang Masalah

Era digital merupakan era teknologi dengan kemajuan yang pesat. Dengan pesatnya penggunaan teknologi informasi dan komunikasi, ancaman siber juga meningkat [1]. Adanya pandemik Covid-19 membuat aktivitas serba dilakukan di rumah sehingga dituntut untuk menggunakan akses internet. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menyatakan 221.563.479 jiwa menggunakan fasilitas internet di Indonesia pada tahun 2024, dari total populasi Indonesia yang mencapai 278.696.200 jiwa pada tahun 2023. Dengan demikian, sekitar 79,5 % dari seluruh penduduk Indonesia menggunakan internet [2]. *Federal Bureau Investigation* (FBI) mengungkapkan tindak kejahatan di dunia siber meningkat menjadi 300 %, serangan umumnya dilakukan pada *server* [3]. *Monitoring server* sangat diperlukan sebagai upaya untuk mengamankan *server*, serangan seperti *malware, bruteforce ssh* dan *web attacks* sangat sering dilancarkan untuk mendapatkan akses terhadap *server* [4].

Penyerang akan mencoba mengeksploitasi kelemahan dalam sistem jaringan untuk mengejar tujuan mereka dengan mengalahkan layanan keamanan yang ada. Karena jaringan publik awalnya dibuat tanpa memperhatikan aspek keamanan, maka serangan dari penjahat siber semakin meningkat dari tahun ke tahun [5]. Oleh karena itu, perlu adanya monitoring pada *server* untuk memastikan data agar tetap aman dari aksi jahat. Untuk melakukan hal ini, perlu digunakan *tools* yang dapat memantau perkembangan pada *server*, Salah satu alat yang berfungsi untuk monitoring *server* yaitu *Wazuh* [3]. Adapun untuk meningkatkan keamanan server juga bias dikombinaskan dengan system honeypot yaitu system yang berfungsi untuk membuat layanan palsu. Penerapan sistem Honeypot harus dilakukan dengan cermat dan terpisah dari server asli, hal ini dilakukan untuk menghindari resiko pada *server* asli[6].

Pada pembuatan tugas akhir ini penulis membangun sistem HIDS yang terintregasi dengan *Honeypot* agar sistem tersebut mampu mencegah dan mendeteksi serangan siber secara real time [7]. HIDS menggunakan *wazuh* memiliki kelebihan dalam kelengkapan data hasil deteksi karena diletakkan pada *endpoint server*. Prototipe sistem monitoring tersebut dikembangkan untuk

mempermudah *security analyst* dalam mendeteksi ancaman siber pada *endpoint server*. Prototipe sistem monitoring tersebut dimulai dengan merancang *Wazuh server* dan *Wazuh agent*. *Honeypot* berfungsi untuk membuat akses *server* palsu agar penyerang terjebak dalam sistem tersebut dan dapat dideteksi oleh IDS *Wazuh*.

1.2. Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut:

1. Bagaimana cara mendeteksi serangan siber yang terdapat pada *server*?
2. Bagaimana cara HIDS menentukan serangan siber dengan akurat?
3. Bagaimana cara agar *security analyst* dapat menganalisa ancaman dengan mudah?

1.3. Tujuan dan Manfaat

Adapun tujuan dari Proyek Akhir ini, sebagai berikut:

1. Membuat *Wazuh* sebagai sistem HIDS yang diintegrasikan dengan *Honeypot*.
2. Meningkatkan tingkat akurasi pendeteksian ancaman siber.
3. Mempermudah *security analyst* menganalisa serangan.

Adapun manfaat dari Proyek Akhir ini, sebagai berikut:

1. Dapat menguji sistem dalam mendeteksi segala jenis serangan.
2. *Wazuh* dapat mendeteksi dan mencegah ancaman siber dengan akurat dikarenakan *wazuh* diintegrasikan dengan *Honeypot*.
3. *Security analyst* dapat lebih mudah menentukan ancaman siber dikarenakan *dashboard* menampilkan informasi *alerts* yang jelas.

1.4. Batasan Masalah

Dalam Proyek Akhir ini, dilakukan pembatasan masalah sebagai berikut:

1. Perancangan prototipe sistem monitoring HIDS menggunakan OS *Ubuntu*
2. Setelah *Wazuh* terpasang akan dikombinasikan dengan *Honeypot* untuk menambahkan sistem pencegahan
3. Melakukan simulasi perancangan yang telah dibuat dengan log yang dikirimkan melalui wazuh *agent.*
4. Sistem berjalan selama *server running.*
5. Parameter QOS yang diamati yaitu, *Throughput, packet loss, Delay* dan *jitter*

1.5. Metode Penelitian

Metode penelitian pada tugas akhir ini yaitu :

1. Studi literatur

   Tahap ini dilakukan untuk mengumpulkan informasi dan mempelajari materi-materi yang terkait seperti IDS, *Wazuh, Honeypot* dan serangan siber seperti *bruteforce,* DOS dan *malware*.
2. Analisis kebutuhan sistem

   Metode yang dilakukan adalah mengumpulkan berbagai kebutuhan untuk mengerjakan tugas akhir seperti perangkat untuk implementasi, sistem operasi *Ubuntu* dan *resource* yang dibutuhkan untuk instalasi *Honeypot* dan *Wazuh*.
3. Perancangan sistem

   Hal ini dilakukan dengan merencanakan sistem yang akan dibangun, seperti konfigurasi *Honeypot* dan IDS *wazuh*.
4. Implementasi

   Implementasi dilakukan dengan melakukan pengujian serangan siber meliputi *bruteforce,* DOS dan *malware* terhadap *server*.