BAB I

PENDAHULUAN

1.1 Latar Belakang

Direktorat Inovasi dan Inkubator Bisnis (DIIB) ialah sebuah unit yang memiliki *Website* dan *Storage* sebagai tempat penyimpanan data-data atau pemberkasan penting namun pada DIIB ini *Website* belum memiliki sistem identifikasi dari aktivitas atau serangan mencurigakan dari luar. Oleh karena Itu belum adanya sistem identifikasi di DIIB belum dapat mendeteksi serangan dari luar ataupun aktivitas yang mencurigakan. Salah satu serangan yang terjadi yaitu halaman *website* yang mendadak berubah ketika dibuka, serta munculnya iklan yang menganggu hingga perubahan tampilan *website* secara keseluruhan (Anif et al., 2015) .

Oleh karena permasalahan diatas, peneliti berupaya mencari solusi dengan cara menerapkan *Intrusion Detection System* (IDS) sebagai sistem yang memonitoring trafik jaringan untuk mendeteksi aktivitas mencurigakan atau akses yang tidak sah menggunakan *Portsentry*. Hal pertama yang harus dilakukan dalam menerapkan IDS ialah menginstal *ubuntu* terlebih dahulu sebelum menggunakan *Portsentry* sebagai *tools* yang digunakan untuk menghindari berbagai aktivitas *scanning* dan mendeteksi adanya *port scanning* serta merespon secara aktif serangan dari luar. Setelah IDS berhasil dijalankan dengan menggunakan *Portsentry* dan ditemukan aktivitas yang mencurigakan maka sistem tersebut akan memberikan laporan dalam bentuk peringatan. Dalam hal ini *Portsentry* akan secara

aktif memblokir IP atau *server hacker* tersebut secara otomatis. Tujuannya adalah agar *website* DIIB aman dari akses yang dilakukan oleh pihak yang tidak berkepentingan (Fauzi et al., 2023a)

PortSentry tersedia untuk berbagai platform Unix, termasuk Linux, *OpenBSD & FreeBSD*. Versi 2.0 dari *PortSentry* memberikan cukup banyak fasilitas untuk mendeteksi scan pada berbagai mesin *Unix*. Versi 1.1 mendukung mode deteksi yang klasik Portsentry yang tidak lagi digunakan pada versi 2.0. PortSentry 2.0 membutuhkan library libpcap untuk dapat di jalankan, biasanya sudah tersedia berbentuk *RPM* dan akan di *install* secara automatis jika menggunakan *Linux Mandrake*. Dan disini peneliti memilih menggunakan Portsentry dari *OS linux* Ubuntu dikarenakan lebih mudah untuk menjalankannya (Muh Mashuri Mustofa, 2013)

Portsentry merupakan salah satu *Intrusion Detection System* (IDS) yang dibuat dengan cara *Menginstal* Ubuntu terlebih dahulu dan mengkonfigurasi *Portsentry* setelah penginstalan berhasil. Keunggulan menggunakan *portsentry* sebagai fitur utama dalam mendeteksi dan merespon serangan dari luar yaitu dimana Portsentry dapat mendeteksi berbagai serangan *scanning*, bereaksi terhadap usaha *port scan* dari luar dengancara memblokir penyerangan secara *real time* dari usaha *scanner* maupun sistem,melaporkan semua kecurigaan dan pelanggaran,mengingat alamat IP penyerang jika ada serangan port scan yang bersifat random maka portsentry akan bereaksi, dan *portsentry* dirancang agar mudah di konfigurasikan dan bebas dari pemeliharaan (Ulfa et al., 2012).

Berdasarkan uraian diatas terkait permasalahan keamanan *website* dan *storage* sebagai penyimpanan data dan berkas penting pada unit Direktorat Inovasi dan Inkubator Bisnis (DIIB) terkhususnya *web server* yang sering di akses dengan tidak hati-hati seperti penyusupan *website* yang mana keamanan data penyimpanan yang disimpan melalui *web* tersebut. Untuk itu peneliti menerapkan IDS dengan menggunakan *Portsentry* untuk memonitoring serangan atau aktivitas-aktivitas mencurigakan. Oleh karena itu, peneliti mengambil judul "**Penerapan IDS (Intrusion Detection System) di Direktorat Inovasi dan Inkubator Bisnis Menggunakan Portsentry**"

1.2 Rumusan Masalah

Dari latar belakang yang telah dikemukan di atas, maka rumusan masalah dari penelitian ini adalah bagaimana menerapkan IDS menggunakan *Portsentry* untuk mendeteksi adanya serangan atau aktivitas dari luar di Direktorat Inovasi dan Inkubator Bisnis (DIIB).

1.3 Batasan Masalah

Agar penelitian ini lebih terfokus, maka terdapat beberapa masalah sebagai berikut:

1. Penerapan IDS menggunakan *Portsentry* untuk mendeteksi aktivitas mencurigakan dalam sebuah sistem *Website* dan *Storage* di Direktorat Inovasi dan Inkubator Bisnis (DIIB)
2. *Portsentry* sebagai IDS yang akan bereaksi secara *Real Time* (langsung)

apabila terdapat serangan dari luar dengan cara memblokir *IP Address* penyerang dan memasukan ke *file* yang digunakan sebagai laporan.

3. IDS *(Intrusion Detection System)* dengan menggunakan Portsentry dapat memberikan sebuah laporan berbentuk peringatan atau notifikasi apabila ditemukan aktivitas.

1.3 Tujuan penelitian

Berdasarkan judul yang dikemukan peneliti, maka tujuan dari penelitian ini adalah sebegai berikut:

1. Untuk mengetahui serangan atau aktivitas yang mencurigakan maka dilakukannya perancangan IDS menggunakan *Portsentry* di Direktorat Inovasi dan Inkubator Bisnis (DIIB).
2. Untuk menerapkan IDS menggunakan *Portsentry* di Direktorat Inovasi dan Inkubator Bisnis (DIIB).
3. Untuk mendeteksi adanya serangan dan aktivitas-aktivitas mencurigakan yang ada di *Website* Direktorat Inovasi dan Inkubator Bisnis (DIIB)

1.4 Manfaat Penelitian

Dengan dilaksanakan penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Mengetahui bagaimana cara menerapkan IDS (*Intrusion Detection System*) menggunakan *Portsentry* di Direktorat Inovasi dan Inkubator Bisnis (DIIB).
2. Menerapkan IDS *Portsentry* sebagai media pendeteksi aktivitas

mencurigakan atau akses yang tidak sah pada Direktorat inovasi dan Inkubator Bisnis (DIIB).

3. Mengetahui adanya aktivitas atau serangan dari luar pada Direktorat Inovasi dan Inkubator Bisnis (DIIB).

1.5 Penelitian Terdahulu

Berikut ini adalah penelitian terdahulu yang masih relevan dengan topik yang penulis bahas.

Pertama penelitian yang dilakukan oleh Muhammad Anif,Sindung HWS dan Mokhamad Daman Huri, peneliti melakukan Perancangan IDS server dengan menjadikan kampus politeknik semarang sebagai objek penelitian. IDS server yang dirancang ini ditunjukan untuk mahasiswa dan dosen pada kampus tersebut. Peneliti juga menjadikan portsentry sebagai Antarmuka. Metode yang digunakan pada penelitian ini meliputi kerangka kerja yang terdiri dari mendefinisika masalah, Analisis masalah, Menentukan tujuan penelitian, studi literature,desain dan implementasi . hasil dari penelitian ini peneliti berhasil merancang IDS server pada jaringan lokal dikampus politeknik semarang dan melakukan pendeteksi ke portsentry dimana sistem akan memblokir serangan port scanning yang dianggap sebagai tindakan berbahaya (Fauzi et al., 2023b).

Kedua, peneliti yang dilakukan oleh Muh Masruri Mustofa, Eko Aribowo.Pada penelitian ini,peneliti melakukan penerapan sistem keamanan jaringan nirkabel hostspot menggunakan metode yang digunakan adalah studi pustaka *(Library Research)* dan observasi yaitu melakukan pengamatan secara

langsung terhadap jaringan hotspot di UAD. Analisis dilakukan untuk mendapatkan hasil serta data yang bisa dijadikan sebagai acuan guna menerapkan suatu sistem keamanan jaringan hotspot berbasis honeypot dan Beta test. Hasil penelitian ini adalah kombinasi antara *Honeypot* dan IDS dengan *Honeyd* dan *Snort* ini memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditunjukan ke jaringan hotspot (Ulfa et al., 2012).

Ketiga, penelitian yang dilakukan oleh Khairil, Toibah Umi Kalsum. Dalam sebagai keamanan *web server* yang mana Jenis penelitian ini adalah mampu menghadapi ancaman *firewall* terhadap sistem keamanan *web server*. Pada penelitian ini melalui celah keamanan yang berperan sebagai pemberi peringatan adanya ancaman. Penelitian ini dilaksanakan dengan beberapa tahapan. Hasil dari penelitian ini adalah aplikasi snort berfungsi sebagai *network intrusion detection system* dalam mendeteksi penyusupan yang melakukan *scanning port.* Snort menampilkan peringatan ancaman secara *real time* dalambentuk tanggal, waktu 2 menit. file log ini sebagai analisa bagi administrator jaringan untukmeningkatkan keamanan terhadap *web server* (Firdaus & Informatika, 2020).