BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Pada saat sekarang ini teknologi semakin berkembang seiring berjalannya waktu. Dengan kemajuan teknologi yang semakin pesat pada saat sekarang ini masyarakat harus mengikuti perkembangannya karena teknologi pada saat sekarng ini sangat membantu berbagai kegiatan masyarakat baik dalam pekerjaan rumah tangga, dan lainnya. Pada zaman yang semakin canggih tentunya masyarakat juga sangat memiliki ketergantungan yang tinggi terhadap teknologi terutama disaat melakukan transaksi secara *online*, tentu sangat banyak data yang tersebar melalui jaringan internet. Tidak dapat dipungkiri juga dengan adanya ancaman kejahatan yang akan ditemui seperti *virus, malicious, trojan, worm, DOS, hacker, spoofing, sniffing, spamming, cracker* dan lainnya, yang membuat tidak nyaman saat menggunakan media yang terhubung dengan jaringan internet serta mengancam sistem dan data yang terdapat didalamnya.

RSUD Lubuk Basung sudah menjadi kepercayaan untuk masyarakat sekitar dalam pelayanan kesehatan. Pada RSUD terdapat sistem informasi yang terbilang sangat kompleks. Dengan kompleksitas yang dimiliki ini, maka menambahkan resiko yang dimiliki oleh sistem informasi RSUD Lubuk Basung. Melihat pentingnya data di dalam sistem informasi RSUD Lubuk Basung, maka pengelolaan keamanan TI pun perlu diperhatikan. Untuk menghadapi masalah keamanan jaringan juga dapat menggunakan *firewall*. Saat ini *firewall* yang ada dirasa kurang baik dalam melakukan pendeteksian penyusupan oleh karena

firewall dirancang untuk memblok suatu aktivitas dimana penyusupan dilakukan secara tegas. Sistem pendeteksian *Intrusion Detection System (IDS)* memegang peranan penting dalam pengamanan jaringan. *PSAD (Port Scan Attack Detector)* dan *FWSNORT (Firewall Snort)* merupakan produk Open Source yang menjadi kombinasi pilihan sebagai pendeteksi intrusion dalam jaringan yang dapat dikembangkan menjadi *Intrusion Prevention System (IPS)*. Intrusion Prevention *System* ini akan dikombinasikan dengan kemampuan *honeypot* untuk melakukan pencegahan maupun melihat aktivitas *attacker*. Dalam penelitian ini penulis merancang dan membangun sistem IPS dikombinasikan dengan *honeypot* agar dapat menangani suatu penyerangan berdasarkan pada alert yang telah ditampung dalam file log dan juga dapat memberikan log tentang serangan yang baru dan belum diketahui oleh sistem IPS.

Perkembangan teknologi dalam jaringan komputer lambat laun semakin pesat seiring dengan meningkatnya kebutuhan akan akses jaringan yang efisien , stabil dan cepat serta kemanan yang handal. Salah satu faktor yang mempengaruhi kualitas dalam jaringan adalah network security atau keamanan jaringan, banyak teknik yang dapat dilakukan dalam meningkatkan keamanan jaringan, baik dengan membangun sistem *firewall*, dengan menggunakan layer7 protocol maupun dengan *port* security, *port* security memanfaatkan *port-port* yang ada untuk mengizinkan akses ke jaringan, *switch port* security merupakan suatu kemampuan perangkat *switch* untuk mengamankan jaringan LAN (Local Area Network) terdapat beberapa jenis *switch port* security yang digunakan yaitu default/ static *port* security, *port* security dynamic learning dan sticky *port* security, penulis akan melakukananalisis terhadap masing-masing jenis *switch*

port security untuk menentukan kehandalan,kegunaan dan pemanfaatannya dilapangan.(Lukman & Bachtia, 2016)

Pada penelitian sebelumnya yang dilakukan oleh Risa Eri Susanti, dkk. pada tahun 2020 dengan judul *Implementasi Intrusion Prevention System (IPS) OSSEC* dan *Honeypot Cowrie*.Penelitian ini bertujuan untuk mengetahui akurasi deteksi penyerangan terhadap sistem seperti pemalsuan data hingga merusak sistem maupun jaringan. Dengan adanya permasalahan tersebut, dibutuhkan sistem pengamanan berlapis untuk menjaga integritas data maupun sistem agar tetap utuh. Pengamanan sistem *OSSEC* yang diintegrasikan dengan *honeypot cowrie* ini bertujuan untuk menekan waktu penyerangan, dimana pada sistem ini saling bekerja sama untuk memberikan log untuk melakukan tindakan terhadap penyerang. *OSSEC* bekerja layaknya *firewall* yang dapat melakukan *allow* maupun *block*. Sedangkan *honeypot cowrie* ini bekerja layaknya *server* asli untuk menjebak penyerang seolah-olah berhasil melakukan penyerangan. Dalam penelitian ini, sistem yang telah dirancang agar dapat menangani adanya serangan seperti *Port Scanning, SSH brute force, Man in The Middle (MITM) attack, dan Distributed Denial of Service (DDoS)*. Dari hasil perbandingan serangan dengan *confusion matrix* ini *OSSEC* yang diintegrasikan dengan *honeypot cowrie* memiliki tingkat akurasi yang besar terhadap serangan *DDoS,* Berdasarkan log, akurasi deteksi dapat mencapai persentase 100%.(Susanti et al., 2022)

Pada penelitian sebelumnya yang dilakukan oleh Bagas Suryo Anggoro, dkk. tahun 2019 dengan judul *Implementasi Intrusion Prevention System Suricata* dengan *AnomalyBased* untuk Keamanan Jaringan PT. Grahamedia Informasi. Penelitian ini menjelaskan tentang sistem yang bertujuan mengimplementasikan

Intrusion Prevention System (IPS) yang memanfaatkan *firewall* sehingga dapat mendeteksi serangan yang berbasis *port* dan protokol dan menolak akses, serta mencatat log yang teridentifikasi negatif. Hasil penelitian ini adalah Suricata bekerja berdasakan *anomaly-based*, setiap paket yang masuk diseleksi menggunakan rules Suricata dengan membandingkan aktivitas yang sedang di-monitoring dengan aktivitas atau kondisi biasa sebelum di-monitoring untuk mengetahui adanya anomali pada jaringan. Selain itu, hasil dari penelitian ini ditemukan beberapa anomali antara lain SQL Injection dan login SSH sebagai admin dengan perangkat lain (Anggoro & Sulistyo, 2019).

Pada penelitian sebelumnya yang dilakukan oleh Farid Wahyudi, dkk. Pada tahun 2021 dengan judul *Perancangan Security Network Intrusion Prevention System* Pada PDTI Universitas Islam Raden Rahmat Malang. Penelitian ini bertujuan mengembangkan sebuah keamanan jaringan menggunaan pendekatan IPS khususnya pada PDTI Universitas Islam Raden Rahmat Malang, karena banyak pengakses yang mengunjungi situs kampus baik intranet maupun internet sehingga sebagai unit pengelola jaringan kampus ingin memberikan keamanan yang maksimal. Tercatat kurang lebih 1000 pengunjung situs kampus perharinya membuat rawan terhadap intrusi. Oleh karena itu perancangan *monitoring* dan *security network* IPS diharapkan bisa memberikan jaminan keamanan jaringan khusunya PDTI Universitas Islam Raden Rahmat Malang.(Farid & Listanto, 2021)

Pada penelitian sebelumnya yang dilakukan oleh Rizka Albar, dkk. Pada tahun 2022 dengan judul *Analisis keamanan jaringan menggunakan metode sniffing dan implementasi keamanan jaringan pada mikrotik router os v6.48.3*

menggunakan metode port knocking. Penelitian ini bertujuan untuk mengetahui tingkat keamanan jaringan beserta meningkatkan keamanan jaringan untuk menghindari dari pihak yang tidak bertanggung jawab untuk melakukan pencurian data *(Attecker)*. (Albar & Putra, 2022)

Pada penelitian sebelumnya yang dilakukan oleh Sutarti, dkk. Pada tahun 2018 dengan judul *Implementasi IDS (intrusion detection system)* Pada sistem keamanan jaringan Sman 1 cikeusal. Penelitian ini bertujuan untuk mengetahui sebuah sistem *Intrusion Detection System (IDS) snort* dapat mendeteksi adanya serangan dan penyalahgunaan jaringan, selanjutnya untuk mengetahui penganalisaan *log* yang dihasilkan sebagai peringatan kepada *administrator*, dan yang terakhir yaitu untuk mengetahui *PfSense* dapat melakukan tindakan lanjut terhadap *alert* yang dihasilkan oleh *snort*.(Pancaro & Saputra, 2018)

Pada penelitian yang dilakukan oleh Ernawati, dkk. Pada tahun 2019 dengan judul *Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector, Portsentry, and Suricata*. Penelitian tersebut bertujuan untuk menganalisis kinerja IDS (PSAD, *Port*sentry dan Suricata). Metode yang digunakan yaitu *NDLC (Network Development Life Cycle)* dimana Sistem mendeteksi dan memantau jumlah aktivitas mencurigakan yang terjadi di *server* atau jaringan komputer. Jika terjadi ancaman maka sistem akan memberikan peringatan dan menyimpan catatan untuk dianalisis. (Ernawati et al., 2019).

Instrusion Detection *System* atau IDS adalah suatu sistem aplikasi yang dapat memonitor lalu lintas jaringan dari paket-paket data yang mencurigakan atau yang melanggar aturan keamanan jaringan dan kemudian membuat laporan dari aktivitas jaringan tersebut (Suhartono & Abd.Rahman Patta, 2017).

Intrusion Prevention *System* atau IPS adalah sistem yang dapat secara otomatis mendeteksi aktivitas mencurigakan yang berpotensi berbahaya dalam jaringan. Cara kerja dari IPS dimulai dengan memindai paket yang datang dari luar jaringan, IPS mempunyai file konfigurasi yang berisi rule-rule untuk mengidentifikasi paket yang aman dan tidak. Ketika suatu paket yang masuk terdeteksi tidak aman, maka paket tersebut akan dihapus dari jaringan.Selanjutnya IPS akan memberikan peringatan kepada administrator tentang aktifitas yang dilakukan oleh IPS (Santoso et al., 2022).

Honeypot adalah sistem komputer di Internet yang secara tegas diatur untuk menarik dan menjebak orang yang mencoba menembus sistem komputer orang lain. *Honeypot* juga merupakan *server* yang terhubung ke internet yang dirancang khusus untuk memikat para peretas dan penyusup potensial untuk memantau aktivitas mereka dan mengamati bagaimana mereka membobol sistem komputer. Mereka diatur untuk memikat dan menarik orang lain yang ingin menyerang sistem komputer pengguna online (Ravji & Ali, 2019).

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu **”IMPLEMENTASI *HONEYPOT* DENGAN *FWSNORT (FIREWALL SNORT)* DAN *PSAD (PORT SCAN ATTACK DETECTOR)* SEBAGAI *INTRUSION PREVENTION SYSTEM* UNTUK KEAMANAN JARINGAN PADA RSUD LUBUK BASUNG”.**

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dapat disimpulkan permasalahan yang akan dibahas pada laporan ini sebagai berikut :

1. Bagaimana penerapan *FWSNORT (Firewall Snort)* dan *PSAD (Port Scan Attack Detector)* sebagai Instrusion Detection *System* dapat mendeteksi serangan ?
2. Bagaimana pengujian Intrusion Prevention *System* dikombinasikan dengan *honeypot* agar dapat menangani suatu penyerangan ?
3. Bagaimana dengan adanya *FWSNORT (Firewall Snort)* dan *PSAD (Port Scana Attack Detector)* dapat meningkatkan keamanan data pada RSUD Lubuk Basung?

1.3. Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut :

1. Diharapkan hasil penelitian dapat mendeteksi serangan dengan penerapan *FWSNORT* dan *PSAD (Port Scan Attack Detector)* sebagai *Instrusion Detection System (IDS)*

2. Diharapkan hasil pengujian dapat mengatasi suatu penyerangan menggunakan sistem sistem *Intrusion Prevention System (IPS)* dengan *honeypot*

3. Diharapkan dari hasil penelitian, data-data penting yang terdapat pada RSUD Lubuk basung dapat terhindar dari serangan dengan *FWSNORT* dan

PSAD(Port Scan Attack Detector) sebagai *Instrusion Detection System (IDS)*.

1.4. Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka peneliti memberikan batasan masalah yaitu, peneliti akan membuat sistem *Honeypot* yang dipadu dengan IPS menggunakan PSAD dan *FWSNORT* agar memberikan dapat menangani suatu penyerangan berdasarkan pada *alert* yang telah ditampung dalam *file log* dan juga dapat memberikan *log* tentang serangan yang baru dan belum diketahui oleh *system* IPS. IPS berfungsi sebagai sistem yang bekerja memantau aktivitas jaringan yang melalui sistem IPS pada mode inline dan memblokir alamat IP yang mencurigakan setelah data stream dicocokan dengan signature yang ada, sedangkan *Honeypot* bekerja untuk mengetahui aktivitas penyerang dan semua aktivitas yang menuju pada *honeypot* dianggap mencurigakan.

1.5. Tujuan Penelitian

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya adalah:

1. Untuk membantu RSUD Lubuk Basung dalam mendeteksi suatu serangan
2. Untuk membantu pihak RSUD Lubuk Basung dalam menangani suatu serangan

1.6 Manfaat Penelitian

Manfaat dari penelitian ini yaitu :

1. Dengan mendeteksi suatu serangan menggunakan *FWSNORT* dan *PSAD (Port Scan Attack Detector)* dapat membantu RSUD Lubuk Basung mengetahui kualitas keamanan jaringan.
2. Dengan dilakukannya pengujian *Intrusion Prevention System* dikombinasikan dengan *honeypot* dapat menangani suatu penyerangan yang mungkin saja terjadi pada RSUD Lubuk Basung.

1.7 Gambaran Umum Objek Penelitian

1.7.1 Sejarah Singkat RSUD Lubuk Basung

RSUD Lubuk Basung Berdiri pada tanggal 13 Maret 1986. Pada awalnya RSUD Lubuk Basung berdiri sebagai rumah sakit tipe D yang ditetapkan berdasarkan Peraturan Daerah TK II Agam Nomor : 03 Tahun 1994 RSUD Lubuk Basung merupakan RS Tipe D yang mempunyai fasilitas dan kemampuan pelayanan kesehatan dengan pelaksanaan teknisnya Dinas Kesehatan Kabupaten Agam. RSUD Lubuk Basung dipimpin oleh seorang Direktur yang secara teknis bertanggung jawab kepada Kepala Dinas dan secara operasional kepada Bupati selaku kepala daerah.

Pada tanggal 20 Mei 1997 RSUD Lubuk Basung ditetapkan sebagai RSU tipe C sesuai dengan Keputusan Menteri Kesehatan Republik Indonesia Nomor : 482/ Menkes/SK/V/1997 tentang Peningkatan Kelas Rumah Sakit Umum Daerah Lubuk Basung.Seiring dengan semakin besarnya harapan dan tuntutan masyarakat terhadap pelayanan di RSUD Lubuk Basung, maka pada tahun 2015 RSUD Lubuk Basung menjadi PPK-BLUD (Badan Layanan Umum Daerah) Berdasarkan Surat Keputusan Bupati Agam Nomor 477 Tahun 2014 tentang Penetapan Pola Pengelolaan Keuangan Badan Layanan Umum Daerah (PKK-

BLUD) sehingga RSUD Lubuk Basung dapat mengelola keuangan sendiri dengan mengutamakan kelengkapan fasilitas pelayanan demi meningkatkan kepuasan masyarakat terhadap pelayanan kesehatan di RSUD Lubuk Basung.

1.7.2 Profil RSUD Lubuk Basung

Berikut adalah profil RSUD Lubuk Basung :

a. Nama Rumah Sakit : RSUD Lubuk Basung
b. Alamat : Jl. DR. MH. Hatta, Padang Baru,Lubuk Basung, Kabupaten Agam
c. Provinsi : Sumatera Barat
d. Tipe : C

1.7.3 Visi dan Misi RSUD Lubuk Basung

Berikut adalah visi dan misi RSUD Lubuk Basung

a. Visi : Terwujudnya rumah sakit yang profesional, mandiri, inovatif dan berkeadilan
b. Misi :
    1) Mewujudkan rumah sakit yang profesional sesuai dengan standar akreditasi JCI/ISO
    2) Memberdayakan seluruh potensi dan meningkatkan kerjasama untuk mewujudkan kemandirian rumah sakit
    3) Memberikan pelayanan yang inovatif berbasis teknologi terkini
    4) Memberikan pelayanan yang menyeluruh untuk masyarakat tanpa membedakan sastra sosial
c. Motto : Pelayanan tanpa keluhan