BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet telah membantu pengguna untuk mendapatkan informasi secara mudah, salah satu informasi didapatkan dari *website*. *Website* berjalan pada web server, tersedia dari penyedia *hosting* salah satunya yaitu *Virtual Private Server*. *VPS* banyak digunakan untuk *website company profile* dan *e-catalog*, membantu perusahaan menjangkau pasar dan atensi konsumen [1], [2]. Akan tetapi ada risiko keamanan yang mengancam data dan informasi pada web server [3], [4].

Penerapan keamanan server sangat relevan, salah satunya menggunakan *Intrusion Detection System (IDS) Snort* dan *Honeypot Cowrie*, yang akan menjadi keamanan tambahan server. *IDS Snort* akan mendeteksi adanya serangan atau anomali pada jaringan server [5]. Di samping itu *Honeypot Cowrie* akan menjadi peran penting sebagai server palsu, untuk mengelabui penyerang yang mencoba masuk ke server asli [6]. Untuk memaksimalkan dalam menganalisis serangan, akan diintegrasikan dengan *splunk* menggunakan *output plugin alert_json*[7], [8].

Pada penelitian ini melakukan analisis dan implementasi sistem keamanan pada *VPS*, dengan *PPDIOO*. Tahapan dari metode *PPDIOO* yaitu *Prepare (identifikasi kebutuhan VPS), Plan (kebutuhan aplikasi), Design (skema sistem keamanan dan pengujian), Implement (instalasi dan konfigurasi), Operate (Pengujian sistem keamanan),* dan *Optimize (evaluasi sistem keamanan dengan CIA Triad)*. Pendekatan *PPDIOO* yang komprehensif untuk mengimplementasi dan mengelola sistem keamanan secara efektif pada server [9].

Sistem keamanan *IDS Snort* dan *Honeypot Cowrie* yang terintegrasi dengan *splunk*, akan diuji untuk dilakukan evaluasi. Pengujian menggunakan *virtual environment OS Kali* dengan serangan *port scanning, brute force,* dan *DDoS*, data hasil serangan akan dievaluasi dengan standar keamanan *CIA Triad* untuk meningkatkan sistem keamanan yang telah diimplementasikan [10],[4]. Harapan pada penelitian, dapat meningkatkan *awareness* pengguna untuk menjaga data, dan memberikan solusi dalam membangun sistem keamanan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah penulis merumuskan pokok permasalahan sebagai berikut:

1. Bagaimana implementasi *Snort* dan *Honeypot* untuk meningkatkan keamanan, yang terintegrasi dengan *splunk?*
2. Bagaimana data hasil pengujian sistem keamanan dari serangan *port scanning, Brute Force* dan *DDoS* pada VPS Server?
3. Bagaimana hasil evaluasi dari data pengujian dengan standar keamanan *CIA Triad* ,yang dapat memberikan penilaian dan peningkatan pada sistem keamanan ?

1.3 Batasan Masalah

Sejalan dengan apa yang sudah di tuliskan oleh peneliti pada latar belakang, maka dapat ditentukan batasan masalah yang akan dilakukan dalam penelitian ini sebagai berikut:

1. Konfigurasi *Snort* yang terintegrasi dengan *splunk* dan *Honeypot cowrie* yang akan dipasang ke *Virtual Private Server.*
2. Menguji keamanan VPS dengan serangan *port scanning, brute force, dan DDoS,* menggunakan sistem operasi kali yang terinstal pada *virtual environment.*
3. Melakukan pengukuran hasil keamanan dari *Snort* dan *Honeypot* terhadap *VPS* dengan standar keamanan *CIA Triad.*

1.4 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai meliputi:

1. Menguji kemampuan *Snort* dalam mendeteksi serangan dan *splunk* dalam analisis serangan yang akan memberikan informasi ke administrato.
2. Menguji Performa *Honeypot* dalam mendeteksi serangan, mencatat serangan dan melindungi server.
3. Analisa hasil serangan terhadap *Virtual Private Server* dengan CIA triad setelah implementasi *Snort* dan *Honeypot.*

1.5 Manfaat Penelitian

Manfaat yang menjadi alasan dilakukannya penelitian ini adalah sebagai berikut:

1. Mengembangkan keamanan *Virtual Private Server* untuk perlindungan data. Dengan sistem keamanan *IDS* dan *Honeypot*.
2. Peningkatan ketepatan informasi serangan ke Administrator, dengan integrasi *Snort* dan *splunk*.
3. Mengevaluasi hasil dari pengujian serangan *DDoS, Brute Force*, dan *port scanning*

1.6 Sistematika Penulisan

Berisikan sistematika penulisan skripsi yang memuat uraian secara garis besar isi skripsi untuk tiap-tiap bab, dari bab I sampai bab V.

BAB I PENDAHULUAN

Pada bab ini berisi mengenai latar belakang dari pembuatan latar belakang, rumusan masalah, batasan masalah, tujuan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tentang teori-teori dan beberapa elemen unsur yang diperlukan guna berjalannya penelitian ini.

BAB III METODE PENELITIAN

Pada bab ini objek penelitian, alur penelitian, alat dan bahan yang ada pada penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan tentang bagaimana hasil dan pembahasan terkait implementasi IDS *Snort* dan *Honeypot* pada VPS Server beserta pengujian.

BAB V PENUTUP

Pada bab terakhir ini berupa kesimpulan dari penelitian dan juga saran masukan terkait berbagai hal dari implementasi IDS *Snort* dan *Honeypot* sampai pada hasil pengujian, agar bisa disempurnakan oleh peneliti di masa yang akan datang.