BAB I
PENDAHULUAN

1.1. Latar Belakang

Seiring dengan berkembangnya kemajuan teknologi, khususnya dibidang informasi, maka peranan komputer sangatlah penting bagi suatu pemerintahan, pendidikan, maupun perusahaan swasta dalam membantu kegiatan operasional para karyawan dalam melakukan sistem informasi pengolahan data menyajikan suatu informasi yang tepat dan akurat. Sementara itu, masalah keamanan ini masih seringkali kurang mendapat perhatian, seringkali masalah keamanan ini berada diurutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap kurang penting. Apabila menggangu informasi dari sistem, seringkali keamanan dikurangi atau dihilangkan.

Banyak sekali data-data penting yang tersimpan didalam *database server* sebuah *web*. Untuk itu diperlukan suatu sistem keamanan yang canggih untuk mengamankan data-data yang tersimpan di *database server* tersebut. Jika *web server* tidak memiliki sistem keamanan yang canggih maka para peretas atau *hacker* akan dengan mudah mencuri data-data penting yang tersimpan di *database server* tersebut.

Honeypot merupakan sumber sistem informasi data yang bersifat terbuka dan dibuat seolah-olah mirip dengan sistem sebenarnya untuk dikorbankan karena memiliki sumber informasi data palsu untuk menjebak peretas yang akan merusak atau mencuri data dari *server*. Dengan adanya *honeypot,* segala bentuk aktivitas ilegal yang dilakukan oleh peretas dapat digunakan *administrator* sebagai informasi tentang penyerang untuk dianalisis, serta mempelajari aktivitas-aktivitas yang cenderung membahayakan suatu sistem (Hibatul dkk, 2017).

Dinas komunikasi informatika persandian dan statistik kabupaten bekasi saat ini hanya menggunakan *firewall* sebagai sistem keamanan *server* nya. Apabila terjadi peretasan atau aktivitas *hacking* di jaringan lokal atau *intranet,* tentu sangat berbahaya karena dapat dengan mudah melewati *firewall* dan sulit terdeteksi. Dikarenakan pentingnya informasi data yang berada di *server* dinas komunikasi informatika persandian dan statistik dan untuk melindungi *server*

dari serangan orang lain yang tidak memiliki hak akses, maka penulis akan mengimplementasikan sistem keamanan pada *server* diskominfosantik dengan judul "implementasi dan analisis keamanan *server* menggunakan *honeypot cowrie* dengan metode *intrusion detection system snort* (*IDS*)".

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijabarkan diatas dan hubungannya dengan pemilihan judul tersebut, maka penulis merumuskan beberapa pokok masalah yang akan diteliti, yaitu :

1. Bagaimana implementasi sistem *honeypot cowrie* dan *IDS snort* untuk mendeteksi serangan peretas ?
2. Bagaimana pengujian keamanan *server* terhadap serangan yang dilakukan oleh peretas ?

1.3. Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pembahasan masalah dalam penyusunan penelitian ini, maka penulis memberikan batasan masalah, yaitu :

1. Penelitian ini dilakukan di ruang *NOC* (*Network Official Center*) Diskominfosantik Kabupaten Bekasi.
2. Alat untuk membangun sebuah *mini server* menggunakan Raspberry Pi 3 model B+ dengan memori 16GB, *RAM* 1GB dan Sistem Operasi Raspbian Buster untuk Raspberry Pi 3.
3. Jenis *Honeypot* yang digunakan adalah *Cowrie*
4. Jenis *IDS* yang digunakan adalah *Snort*
5. Pengujian terhadap sistem yang diteliti dengan menggunakan *port scanning* dan teknik *brute force attack.*

1.4. Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini, yaitu :

1. Untuk Mengetahui implementasi dari sistem *honeypot cowrie* dan *IDS snort* untuk mendeteksi serangan peretas.

2. Untuk mengetahui cara pengujian keamanan *server* terhadap serangan yang dilakukan oleh peretas.

1.5. Manfaat

Manfaat yang diperoleh dari penelitian ini, yaitu :

1. Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya peningkatan sistem keamanan *server* di Diskominfosantik kabupaten bekasi.

2. Menambah ilmu pengetahuan bagaimana cara untuk mengamankan *server* terhadap serangan yang dilakukan oleh peretas bagi pengembang sistem keamanan *server*.