BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi internet telah menjadikannya sebagai media utama untuk bertukar data. Tidak semua informasi tersedia untuk khalayak umum. Karena internet adalah jaringan komputer publik, tindakan pencegahan ekstra harus dilakukan untuk melindungi data dari pengguna jahat. Seseorang yang ahli dalam meretas atau meretas mekanisme keamanan jaringan komputer disebut sebagai *hacker*. Di beberapa negara, khususnya di Indonesia, ada harapan untuk aplikasi online. Pada tahun 2019, peretas menyerang situs *e-Commerce* Tokopedia, mengakibatkan pembobolan 91 juta data akun, kemudian pada tahun 2021 *hacker* melakukan peretasan lagi, mengakibatkan kebocoran data 279 juta orang Indonesia terekspos dan dijual di dunia maya. Terlepas dari kenyataan bahwa beberapa server telah menetapkan keamanan sesuai dengan persyaratan yang berlaku, mengingat dinamika peretasan global, masih ada risiko peretasan. Keamanan jaringan harus dijaga dari semua jenis serangan, bahkan yang tidak diketahui asal-usulnya. Tindakan sistem sebagai penyerang untuk mendapatkan akses dan data sensitif. Akibatnya, diperlukan sistem yang dapat mengidentifikasi serangan atau mengumpulkan informasi tentang penyerang dan pola intrusi tanpa menyebabkan kerusakan pada server [1].

Honeypot merupakan sistem yang diatur untuk menjadi target peretas, dan juga dapat digunakan untuk mengalihkan serangan ke sesuatu yang lebih penting atau berharga. Sistem tersebut dapat digunakan untuk membantu untuk mengelabui penyerang dalam membobol server [2]. Dalam penelitian, penulis menggunakan HoneyPy sebagai pilihan *honeypot* dikarenakan penulis hanya akan melakukan perbandingan atau pembuktian metode dengan cara menambahkan port yang mudah diserang oleh penyerang sehingga aktivitas ditangkap dengan baik.

Serangan yang paling umum yaitu *Port Scanning* dan *DoS* (Denial Of Service). *Port Scanning* merupakan serangan yang mencoba mendeteksi *port* yang terbuka pada jaringan komputer. Dalam pemindaian dapat digunakan untuk mengidentifikasi kelemahan jaringan komputer. *DoS* merupakan jenis serangan yang melibatkan pengiriman permintaan secara terus-menerus ke server sehingga server tetap sibuk dalam menanggapi *request* yang menyebabkan sistem mengalami kerusakan [3].

Server merupakan sistem komputer yang menyediakan penyimpanan data dan layanan lainnya. Informasi dan bentuk dokumen komplek lainnya merupakan salah satu jenis data yang disimpan di server serta dapat digunakan untuk implementasi sistem *low interaction honeypot* yang dapat ditargetkan tanpa membahayakan server asli. Oleh karena itu, dibangunlah sebuah keamanan yaitu sistem *honeypot* yang dipasang di server untuk berpura-pura sebagai jebakan penyerang dan merekam permintaan yang dimaksud pada Maltrail.

Dalam penelitian ini penulis menggunakan *malicious traffic detection system* (Maltrail) sebagai pilihan untuk mendapatkan aktivitas serangan yang akan dianalisis. Karena merupakan aplikasi yang bersifat *open source* dan semua kejadian yang terdeteksi oleh sensor Maltrail disimpan dalam direktori *logging server* dan juga semua peristiwa yang didapatkan sebelumnya bisa dilihat kembali. Oleh karena itu, penulis memilih Maltrail sebagai pilihan dalam mendeteksi sebuah serangan. Langkah awal yang dilakukan install 3 server yaitu Kali Linux, Linux Mint, dan CentOs dan menerapkan Maltrail yang diberi tidak diberi dan diberi pertahanan menggunakan HoneyPy pada Linux Mint serta mencoba untuk melakukan serangan DoS dengan Kali Linux. Langkah terakhir menganalisis pada bagian Maltrail dengan menggunakan analisis deskriptif. Dengan masih adanya ancaman di dunia maya seperti beberapa situs yang mengalami kebocoran data, tentunya serangan tersebut akan memiliki dampak buruk bagi negara maupun masyarakat. Oleh karena itu, penulis akan mengimplementasikan serta menganalisis bagaimana HoneyPy dengan Maltrail bisa bekerja dengan baik untuk keamanan sebuah server. Pada penelitian ini penulis tertarik untuk menganalisa cara serta mengimplementasikan suatu sistem yang diberi

pertahanan HoneyPy dengan Maltrail sehingga diharapkan dapat menjadi masukan dan solusi untuk menentukan kebijakan keamanan dalam membuat server lebih aman. Berdasarkan hal-hal tersebut penulis akan mengangkat topik ini menjadi tugas akhir dengan judul "Implementasi HoneyPy Dengan *Malicious Traffic Detection System* (Maltrail) Menggunakan Analisis Deskriptif Guna Untuk Mendeteksi Serangan DoS Pada Server".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, adapun perumusan masalah yang berkaitan dengan penelitian yang akan diteliti sebagai berikut:

1. Data dan informasi melalui server rentan untuk diretas meskipun memiliki keamanan *firewall.*
2. Tingkat keamanan yang diberikan oleh *low interaction honeypot.*
3. Penggunaan Maltrail sebagai pendeteksi serangan DoS.
4. Penggunaan HoneyPy dengan maltrail yang di analisis deskriptif.

1.3 Tujuan Penelitian

Tujuan penulis dari penelitian tugas akhir ini yaitu antara lain:

1. Menerapkan HoneyPy dengan Maltrail sebagai metode untuk mengamankan sebuah *server* dari peretasan.
2. Melakukan analisis deskriptif pada Maltrail yang akan dibandingkan sebelum dan sesudah menggunakan HoneyPy.
3. Mendeteksi hasil keseluruhan yang ditangkap pada Maltrail.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini berfokus pada implementasi HoneyPy dengan Maltrail sebagai metode mengamankan sebuah server dari peretasan menggunakan analisis deskriptif dengan sistem operasi LINUX di VirtualBox.
2. Tidak membahas keamanan *firewall* pada sistem.

3. Pengujian dilakukan menggunakan satu laptop pada aplikasi VirtualBox dengan tiga server yaitu Kali Linux sebagai penyerang, CentOs sebagai server dan Linux Mint sebagai server utama yang sudah di Install Maltrail dan HoneyPy.
4. Menggunakan metode *low interaction honeypot*.
5. Membuat secara virtual dan serangan hanya DoS yang dilakukan oleh peneliti.
6. Belum melakukan *pentest,* hanya pembuktian metode.

1.5 Manfaat Penelitian

Manfaat penelitian dalam penyusunan tugas akhir, diantaranya:

1. Bagi penulis, dapat menerapkan *low interaction honeypot* dengan Maltrail menggunakan analisis deskriptif untuk memperoleh hasil analisis keamanan jaringan yang berguna untuk server.
2. Bagi kampus, diharapkan tugas akhir ini dapat dijadikan penelitian lanjutan dan menambah referensi literatur kepustakaan untuk IT Telkom Purwokerto.
3. Bagi masyarakat, diharapkan tugas akhir ini dapat bermanfaat dan dipertimbangkan untuk dikembangkan lebih lanjut.