BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi dalam penggunaan jaringan internet berkembang dengan sangat pesat pada saat ini, bahkan teknologi internet saat ini telah digunakan dari berbagai kalangan baik untuk jejaring sosial, pencarian informasi, maupun kebutuhan lainnya. Internet merupakan kependekan dari *interconnected-networking* yang berarti sebuah sistem jaringan komputer yang beragam dan bersifat global yang terhubung di seluruh dunia. Dalam mengatur integrasi dan komunikasi jaringan komputer ini digunakan protokol yaitu TCP/IP. TCP (Transmission Control Protocol) bertugas memastikan bahwa semua hubungan bekerja dengan benar, sedangkan IP (Internet Protocol) yang mentransmisikan data dari satu komputer ke komputer lain[1]

Jaringan komputer telah menjadi sarana berbagi informasi di seluruh dunia, namun tidak semua informasi tersedia untuk umum. Karena Internet adalah jaringan publik, segala upaya harus dilakukan untuk memastikan keamanan informasi ini. Di sisi lain, ada pihak tertentu yang berusaha menembus sistem keamanan jaringan. Faktor keamanan ini perlu menjadi perhatian khusus karena tidak semua informasi bersifat terbuka dan tidak semua orang dapat mengakses. Pada tahun 2021, ada beberapa kasus kejahatan online yang terjadi salah satunya terhadap properti, seperti komputer atau server jaringan yang termasuk dalam serangan DDOS, peretasan, transmisi virus, siber sampai pelanggaran hak cipta, serta pelanggaran HKI. Pada tahun 2020-2021 selama masa COVID 19, banyak dari masyarakat yang menggunakan jaringan internet sehingga tercatat ada sekitar lima puluh ribu insiden dunia maya, yang mana daerah tertinggi selama periode waktu itu berasal dari Uttar Pradesh dan Karnataka[2]. Dikutip dari website *exabytes.coid,* salah satu kasus *Cybercrime* yang terjadi Indonesia adalah "Kebocoran Data e-HAC Kemenkes (2021)" kasus ini bermula pada Juli 2021 dimana aplikasi Electronic Health Alert (e-HAC) yang

dilakukan oleh Kementerian Kesehatan RI telah menjadi korban serangan siber yang disebabkan oleh peretas. Aplikasi Health Alert Card, aplikasi travel yang wajib dimiliki ini membocorkan data 1,3 juta orang Indonesia. Selain membocorkan data pengguna e-HAC, kasus ini juga mengakibatkan terungkapnya data tes Covid-19 penumpang, data rumah sakit, dan data pegawai e-HAC. Setelah diteliti lebih lanjut, serangan ini terjadi karena kurangnya protokol keamanan aplikasi yang memadai dan penggunaan database *Elasticsearch* yang dianggap kurang aman untuk menyimpan data[3]. Oleh karena itu, dibutuhkannya sebuah solusi untuk dapat meningkatkan sistem keamanan yang dapat mendeteksi serangan serta dapat menjebak penyerang, yaitu dengan membangun sebuah sistem keamanan untuk dapat melengkapi *Network Security Management.*

Berdasarkan beberapa kasus *Cybercrime* yang marak terjadi terutama di Indonesia, untuk dapat menghindari kejahatan yang mungkin dilakukan oleh pihak tertentu, salah satu cara yang dapat dilakukan untuk mengamankan sistem jaringan komputer yaitu dengan mengkombinasikan server atau melibatkan honeypot dalam penanganan sistem dalam sebuah jaringan.

Honeypot yang terpasang pada komputer server dapat dijadikan sebagai pusat data atau informasi yang mirip server asli yang dapat diakses oleh siapa saja termasuk orang-orang yang ingin mencoba-coba mengakses ke dalamnya, karena honeypot ini bersifat terbuka sehingga apapun aktivitas, yang tanpa disadari langsung bahwa komputer server telah merekam segala aktifitas atau kegiatan yang membahayakan yang dilakukan oleh penyusup atau penyerang untuk kemudian dijadi bahan analisis [4].

Upaya yang dapat dilakukan untuk meminimalisir kemungkinan terjadi serangan dalam jaringan komputer saat terkoneksi dengan internet yaitu dengan menambahkan suatu metode yang dapat meningkatkan keamanan jaringan. Salah satu upaya yang dapat digunakan untuk memberikan perlindungan keamanan jaringan yaitu dengan mengembangkan metode honeypot dengan

firewall guna mengimplementasikan *Port Knocking* dan honeypot pada jaringan sistem. Ada beberapa alat yang digunakan untuk konfigurasi dalam implementasi *Port Knocking* dan Honeypot, salah satu alat yang digunakan yaitu virtual dari Oracle VM Virtualbox. Virtualbox merupakan suatu alat perangkat lunak secara Virtualisasi, yang dapat megoperasikan beberapa sistem operasi pada sistem utama. Fungsi ini sangat penting bagi seseorang yang ingin melakukan pengujian dan melakukan simulasi suatu sistem tanpa harus menghapus sistem yang sudah ada sebelumnya [5].

Honeypot merupakan salah satu sistem jaringan yang bisa diimplementasikan untuk mengantisipasi terjadinya *Cyber Crime*. Honeypot honeyd dengan low interaction dilakukan dengan cara interaksi secara tidak langsung kepada penyerang, karena honeyd berperan sebagai umpan atau server bayangan yang memang sengaja untuk diserang sehingga hasil serangan tersebut dapat diketahui dan dianalisa. Pada penelitian ini, honeypot berperan sebagai server bayangan yang menyerupai server sesungguhnya, yang memiliki beberapa layanan disertai portport yang sengaja dibuka untuk diserang. Hasil dari penelitian ini setelah dilakukan pengembangan dapat dianalisis dari adanya kemungkinan kredensial dari penyerang, hal tersebut dapat dilihat dari kenaikan trafik jaringan melebihi batas normal pada sistem monitor, serta dapat dilihat dari file log honeyd secara detail mengenai prilaku apa saja yang telah dilakukan oleh penyerang untuk nantinya dianalisis lalu kemudian dilakukan tindakan pencegahan, serta antisipasi hingga perbaikan baik pada server, sistem jaringan, dan semua layanan yang ada.

Berdasarkan pembahasan diatas, dibutuhkannya sebuah sistem yang mampu mendeteksi dan menangani penyalahgunaan jaringan seperti halnya ancaman yang mungkin terjadi, honeypot low interaction yang memiliki karateristik mudah dan cepat untuk diterapkan menyediakan sistem tiruan yang mana dapat memungkinkan dalam meningkatkan sistem keamanan jaringan komputer atas segala aktivitas ilegal yang dilakukan oleh penyerang, hal tersebut memberikan

informasi tentang penyerang sehingga administrator dapat mempelajari aktivitas yang cenderung membahayakan sistem.

1.2. Rumusan Masalah

1. Bagaimana mengimplementasikan honeyd pada jaringan virtual environment?
2. Bagaimana mengevaluasi keamanan server melalui simulasi serangan DDos?

1.3. Batasan Masalah

Adapun Batasan masalah yang penulis lakukan nantinya adalah sebagai berikut:

a. Implementasi honeyd pada server honeypot.
b. Pembahasan terbatas pada cara kerja honeypot tingkat interaksi rendah (low-interaction honeypot) dalam penggunaan tipe honeyd.
c. Scenario atau simulai pada penelitian ini terbatas pada jaringan local (LAN) yang berada di dalam Virtual Box.
d. PC Server honeypot honeyd menggunakan Ubuntu Server.
e. PC intruder/attacker menggunakan sistem operasi Ubuntu Desktop.
f. Honeypot honeyd menerima serangan dari DDoS berupa ping flooding attack.
g. Penyerangan DDos dengan rentang 10-90 threads.

1.4. Tujuan Penelitian

Tujuan dari penelitian analisis dan implementasi honeypot pada Skripsi ini adalah sebagai berikut:

a. Mengimplementasikan honeypot honeyd pada jaringan lokal.
b. Menguji kemampuan atau kelebihan dari honeypot honeyd jika dilakukan penyerangan.
c. Mengkonfigurasi honeyd untuk meningkatkan keamanan server.
d. Mengevaluasi honeyd melalui simulasi serangan DDos.

1.5. Manfaat Penelitian

Penelitian ini nantinya akan memberikan beberapa manfaat yakni sebagai berikut:

a. Mengetahui lebih mendalam tentang kelebihan honeypot honeyd sebagai pelengkap dalam pengamanan pada sistem jaringan komputer.
b. Lebih memahami Tindakan serta tools yang digunakan yang dilakukan oleh penyusup atau penyerang pada suatu jaringan.
c. Metode honeypot ini dapat membantu sistem keamanan atau administrator jaringan yakni dengan melakukan antisipasi/pencegahan sedini mungkin terhadap penyusup atau penyerang dengan melakukan Analisis file log dari honeyd.