BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Internet adalah jaringan yang menghubungkan berbagai komputer dan jaringan di seluruh dunia dengan berbagai sistem operasi dan aplikasi. dimana hubungan tersebut menggunakan kemajuan perangkat komunikasi modern seperti telepon dan satelit menggunakan protokol konvensional untuk berkomunikasi, seperti protokol TCP/IP. [1]. Hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa jumlah pengguna internet di Indonesia akan mencapai 215,63 juta pada tahun 2022–2023, peningkatan 2,67% dari 210,03 juta pada tahun sebelumnya. Jumlah ini setara dengan 78,19% dari total populasi Indonesia, yang berjumlah 275,77 juta orang. [2].

Semakin banyak pengguna internet, semakin banyak serangan siber yang mengancam komputer, terutama selama pandemi COVID-19. Karena masyarakat dan pemerintah tengah disibukkan dengan meningkatnya kasus virus, pencuri memanfaatkan ketidaktahuan ini untuk melakukan berbagai serangan. Badan Siber dan Sandi Negara (BSSN) mencatat 88 juta serangan siber sejak 1 Januari hingga 12 April 2020 [3]. Menurut Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas). Hal ini pasti sangat mengkhawatirkan bagi banyak orang. Ini karena banyak ancaman yang menyerang *server*, seperti *Brute force*, *Structured Query Language*, dan *Daniel of service*, dapat membuat *server* lumpuh sehingga tidak dapat memenuhi banyak permintaan klien.

Berdasarkan penelitian sebelumnya [4] menyatahkan bahwa Honeypot merupakan sebuah sistem yang di bangun menyerupai dengan sistem yang sesungguhnya dengan tujuan agar para*attacker* teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut. Penelitian ini menggunakan jenis *Honeypot Kippo* yang diimplementasikan supaya mampu memberikan laporan aktivitas serangan *brute force* kepada administrator. Hasil penelitian menunjukkan bahwa implementasi *Kippo* pada sistem dapat membaca setiap serangan dari *attacker* dan mampu mendeteksi

serangan *brute force* sesuai *indicator* serangan yang dicantumkan pada penelitian ini.

Dengan adanya permasalahan di atas, di perlukan sistem keamanan jaringan yang mampu mendeteksi serta mencatat setiap serangan yang dilancarkan oleh *hacker* dengan cepat. *Honeypot* merupakan sebuah sistem yang sengaja di korbankan untuk menjadi sasaran penyerang dengan tujuan dapat mencatat aktivitas serangan yang masuk ke dalam *server* sehingga *server* dapat memperbaiki bagian-bagian yang terkena serangan [5]. Pada penelitian ini, penulis akan melihat kinerja dari kedua jenis *honeypot* yang digunakan yaitu honeypot *Kippo* dan *Dionaea*. Dengan kedua jenis *honeypot* yang berbeda, tentunya keduanya pun memiliki perbedaan dalam hal menangkap aktivitas serangan. Sehingga penulis ingin mengusulkan topik penelitian dengan judul "**ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN *BRUTE FORCE,* DoS DAN SQL *ATTACK* MENGGUNAKAN *HONEYPOT* KIPPO DAN *HONEYPOT* DIONAEA".** Dengan adanya penelitian ini, di harapkan seorang administrator mampu menentukan jenis *honeypot* mana yang lebih baik digunakan dalam mendeteksi serangan sehingga serangan yang masuk ke dalam sistem mampu diatasi secara maksimal.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1) Bagaimana mengimplementasi *Honeypot* Kippo dan *Honeypot* Dionaea pada jaringan *server*?
2) Bagaimana deteksi *Honeypot* dalam menjaga keamanan *server* bila diserang *Brute Force*, DoS dan SQL?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1) Penelitian ini menggunakan aplikasi Oracel VM VirtualBox.
2) Penelitian ini menggunakan sistem keamanan *Honeypot* Kippo dan *Honeypot* Dionaea.
3) Pengujian serangan *Blute Force* dilakukan dengan *medusa* sebagai alat untuk mencari kombinasi *username* dan *password.*
4) Pengujian serangan Dos *Attack* menggunakan LOIC.

5) Pengujian serangan SQL Injection menggunakan SQLMap.
6) *Honeypot* Kippo dapat mencatat aktifitas dari serangan ssh.
7) *Honeypot* Dionaea dapat mencatat log dari hasil penyerangan Dos *Attack.*
8) Hanya membaca serangan *Brute Force,* Dos dan SQLMap *Attack*.
9) Pengumpulan data menggunakan analisis *log.*
10) Sqlmap hanya sebagai ujicoba serangan *database* yang terdapat pada server.

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah:

1) Dapat mengimplementasi *Honeypot* Kippo dan *Honeypot* Dionaea pada jaringan *server*.
2) Dapat mendeteksi serangan terhadapat *Brute Force,* Dos dan SQL *Attack*.

1.5 MANFAAT PENELITIAN

Pada penelitian ini diharapkan mampu membantu meningkatkan keamanan sistem dan jaringan serta mengamankan *server* dari serangan siber seperti peretasan, *malware* dan serangan *Daniel of service* sehingga membantu melindungi sistem dan layanan dari kerusakan dan penyalahgunaan.

Keamanan jaringan penting untuk melindungi data sensitif, termasuk informasi pribadi, informasi bisnis, dan data kritikal serta diharapkan mempermudah seorang administrasi dalam mendeteksi atau memonitoring *server* saat terjadinya serangan siber.

1.6 SISTEMATIKA PENULISAN

Beberapa bab membentuk penulisan skripsi ini. Bab I membahas latar belakang, rumusan masalah, batasan masalah, tujuan penulisan, keuntungan, dan sistematika penulisan. Bab II memberikan uraian tentang penelitian pustaka dan dasar teori yang dapat mendukung analisis penelitian. Bab III membahas metode penelitian, skenario penguji, dan perangkat atau alat yang digunakan. Bab IV memberikan hasil dan pembahasan tentang analisis keamanan jaringan terhadap serangan brute force dan serangan dos menggunakan honeypot kippo dan honeypot di. Bab V merupakan isi dari kesimpulan dan saran yang akan diteliti.