BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Website saat ini berfugsi sebagai layanan utama untuk mencari informasi, memperkenalkan produk, jasa, pengiklanan, tempat dilakukannnya jual beli dan masih banyak lagi fungsi yang dapat dimanfaatkan [1]. Untuk melakukan pelayanan dari permintaan pengguna, *website* memiliki penyedia layanan akses yang disebut dengan *web server*. Selain sebagai penyedia layanan, *web server* juga menjadi wadah dari informasi penting yang ada pada suatu *website*. Oleh karena itu, *webserver* menjadi tempat yang paling rawan dilakukan penyerangan. Penyerang akan melakukan serangan guna untuk mendapatkan akses ilegal yang dapat membahayakan sistem informasi yang bersifat penting dan privasi [2]. Oleh karena itu, keamanan pada jaringan terus dikembangkan, terutama oleh *system administrator* yang bertugas untuk mengamankan sebuah server pada keamanan *server*. Terbukanya *port* pada *server* untuk layanan yang bersifat *public* maupun *privat* menjadi celah dilakukanya penyerangan [3].

Port knocking merupakan sebuah metode yang digunakan untuk mengamankan jaringan. Cara kerja dari metode ini yaitu melalui *port* yang tertutup dengan metode otorisasi *user* berdasarkan *firewall* untuk melakukan komunikasi. *Port knocking* akan menutup masing-masing *port* yang ada dan port yang sudah diberikan aturan ketukan yang diketahui oleh pengguna tertentu yang dapat membukannya menggunakan aturan ketukan [4]. *Port logic* yang digunakan untuk *web server* yaitu *port* 80. Sedangkan *honeypot* merupakan sumber sistem informasi data yang dibuat seakan-akan mirip dengan sumber aslinya dan bersifat terbuka yang dikorbankan untuk diserang. Hal tersebut bertujuan untuk menjebak penyerang agar tidak masuk pada sumber yang sebenarnya. Selain itu, metode *honeypot* juga dapat mendeteksi aktivitas apa saja yang dilakukan oleh penyerang. Sehingga, *administrator* dapat menganalisis dan mempelajari aktivtas apa saja yang dilakukan penyerang dan cenderung dapat membahayakan sistem informasi [5].

Penelitian oleh Wilman, dkk. [3] yang dilakukan pada tahun 2018 melakuanan penelitian menggunakan metode *port* knocking dan honeypot sebagai keamanan jaringan pada server ubuntu virtual. Namun pada penelitian tersebut penulis tidak melakukan analisis potensi serangan yang jelas terhadap metode *port knocking* dan *honeypot* yang diimplementasikan, yang mengakibatkan . Sehingga, pada penelitian ini penulis akan melakuan pengujian menggunakan serangan *port scaning* dan *brute force*. Menurut permasalahan yang sudah diuraikan tersebut, maka penulis mengusulkan untuk mengkombinasikan metode *port knocking* dan *honeypot,* sehingga penulis mengambil judul sebagai tugas akhir yaitu **"KEAMANAN JARINGAN MENGGUNAKAN KOMBINASI METODE *PORT KNOCKING* DAN *HONEYPOT*".**

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1) Bagaimana performansi dari kombinasi metode *port knocking* dan *honeypot* sebagai keamanan jaringan untuk mengatasi serangan *brute force* dan *port scanning*?
2) Bagaimana implementasi dari kombinasi metode *port knocking* dan *honeypot* pada *web server*?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1) Proses pengkombinasian metode *port knocking* dan *honeypot.*
2) Implementasi metode *port knocking* dan *honeypot* pada *web server*.
3) Proses pengujian pada kombinasian metode *port knocking* dan *honeypot* pada *web server*.
4) Jenis serangan yang dilakukan sebagai bahan uji adalah *port scaning* dan *brute force.*
5) Jenis sistem keamanan jaringan yang dibahas hanya *port knocking* dan *honeypot.*
6) Penelitian yang akan dilakukan hanya mencakup pada jaringan lokal menggunakan jenis topologi LAN.

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1) Menganalisis performansi dari kombinasi metode *port knocking* dan *honeypot* terhadap serangan *port scanning* dan *brute force*.
2) Mengimplementasikan kombinasi metode keamanan jaringan *port knocking* dan *honeypot* pada *web server*.

1.5 MANFAAT

Manfaat dari penelitian ini adalah memberikan panduan atau referensi kepada *system administrator* khususnya pada pengelolaan *web server* dalam melindungi data atau informasi penting yang dapat disalah gunakan oleh pihak yang tidak bertanggung jawab.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian ini dibagi manjadi 3 bagian:

1. BAB 1 : PENDAHULUAN

   Bagian pendahuluan berisi mengenai latar belakang, rumusan masalah yang diangkat, manfaat dan tujuan penelitian.
2. BAB 2 : DASAR TEORI

   Pada bagian ini membahas teantang kajian pustaka serta dasar pustaka yang menjadi landasan reverensi penulis dalam menyusun penelitian ini.
3. BAB 3 : METODE PENELITIAN

   Pada bagian membahas mengenai alat yang digunakan, spesifikasi perangkat yang digunakan dan diagram alur penelitian.