BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komunkasi berkembang pesat disertai dengan kasus kejahatan pada internet yang semakin berkembang. Kebutuhan dan penggunaan terhadap teknologi informasi yang diterapkan pada internet dalam banyak hal, seperti *e-mail*, *e-education, e-government* dan lain sebagainya. Pemanfaatan internet yang menjadikan komunikasi antar manusia menjadi efisien dan mudah. Dengan semakin tingginya kebutuhan penggunaan internet semakin meningkat pula ancaman yang ada di internet (Handoyo et al., 2016).

Sistem keamanan pada sebuah server yang masih lemah memungkinkan banyak penyusup yang memasuki celah keamanan pada server. Peningkatan keamanan server diperlukan agar dapat meminimalisir kemungkinan penyerangan pada sebuah sistem server. Sebuah server dapat mengalami percobaan serangan brute force, serangan ini umumnya memanfaatkan celah layanan FTP dan SSH secara terus-menerus melakukan penyerangan percobaan login dengan username dan password dengan menggunakan database secara umum. Masalah itu mengakibatkan admin server untuk memiliki Intrusion Detection System pada setiap jaringan server. IDS (Intrusion Detection System) adalah software yang bekerja secara otomatis untuk melakukan monitoring pada setiap sistem komputer.

Pada data yang dihimpun dari 1 Januari 2020 sampai dengan 1 April 2020, BSSN melalui website (https://honeynet.bssn.go.id/) telah mencatat adanya serangan ke Indonesia dengan jumlah mencapai 41.645.908 serangan, dimana negara terbanyak yang menyerang ke server Indonesia adalah Irlandia diikuti India, Indonesia dan Rusia.

Pada penelitian Muhammad Iqbal (Muhammad Iqbal, Arini MT, 2020) menggunakan Honeypot Cowrie untuk mengalihkan server port ke port palsu, konfigurasi dilakukan dengan tetap membuka port default SSH pada server. Port Cowrie tidak terdeteksi oleh nmap.

Berdasarkan uraian masalah keamanan tersebut, penulis mengimplementasikan aplikasi *Intrusion Detection System* dengan judul "Implementasi Honeypot Cowrie Sebagai Alat Pertahanan Terhadap Serangan Di Port SSH Dan Menggunakan Telegram Sebagai Notifikasi". Cowrie adalah pengembangan lebih lanjut dari aplikasi Honeypot lainnya yaitu Kippo. Cowrie mendapat update fitur dan menyediakan emulasi yang merekam kegiatan penyerang. Honeypot membuat penyusup server seolah-olah memasuki server asli yang pada praktiknya penyusup memasuki server palsu yang disediakan oleh Cowrie, semua kegiatan pada penyusup pada server palsu direkam termasuk mengenai informasi penyerang. Penggunaan Cowrie dan Telegram manjadi solusi untuk keamanan jaringan yang lebih baik dan sebagai alat pengumpulan data penyerangan pada sistem, notifikasi pada Telegram akan diinformasikan secara otomatis apabila terjadi serangan pada server.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, masalah penelitian ini yaitu sebagai berikut:

1. Bagaimana implementasi Honeypot sebagai keamanan jaringan pada sistem server?
2. Bagaimana Analisa serangan pada honeypot cowrie?

1.3 Tujuan Penelitian

Berikut adalah tujuan dari penulisan tugas akhir ini, yaitu :

1. Merancang sistem dengan Honeypot Cowrie untuk melakukan mitigasi sistem dari penyerangan *brute force* pada port SSH.
2. Mengetahui efisiensi Honeypot Cowrie dalam melakukan mitigasi sistem dari serangan *brute force.*
3. Mengetahui tingkat ketahanan server terhadap serangan *brute force* .

1.4 Batasan Masalah

Agar permasalahan di atas tidak terlalu meluas, oleh sebab itu Penulis memberikan batasan terhadap permasalahan sebagai berikut:

1. Jenis serangan yang digunakan untuk menguji sistem difokuskan pada *brute force* SSH.
2. Penelitian ini masih menggunakan *virtual* server
3. Sistem pada penelitian ini hanya menggunakan *software Ubuntu*.
4. Sistem jaringan ini masih belum sempurna.

1.5 *State Of The Art* Bidang Penelitian

Implementasi dari honeypot sebagai salah satu alternatif untuk mengamankan jaringan telah dipakai dan dibuktikan oleh beberapa penelitian yang telah berhasil dilakukan sebelumnya.

Pada penelitian yang dilakukan (Muhammad Iqbal, Arini MT, 2020) Pengamanan server Ubuntu dengan metode port knocking dengan otentikasi sebagai syarat untuk menggunakan port service, hanya pengguna yang diperbolehkan saja untuk mengakses port dan dengan menggunakan Honeypot sebagai server tiruan pada metode port knocking, dapat mengalihkan port service kepada fake port yang dibuat honeypot. Kemudian, penelitian Fahana (Fahana et al., 2017) analisa dilakukan dengan menunjukkan bahwa IDS yang dirancang telah berhasil mendeteksi serangan dengan memanfaatkan Snort. Alert berkerja dengan sangat baik dan mampu mengirimkan informasi ke database yang selanjutnya informasi diteruskan dengan menggunakan aplikasi instant messenger telegram secara real time. Hasil menunjukkan bahwa telah terjadi serangan ddos melalui ICMP berdasarkan analisa log yang dilakukan.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini adalah sebagai berikut:

BAB 1. PENDAHULUAN

Berisi latar belakang, perumusan masalah, tujuan penulisan, *state of the art* bidang penelitian, dan sistematika penulisan.

BAB 2. TINJAUAN PUSTAKA

Berisi referensi pustaka untuk mendukung penulisan Tugas Akhir. Dianjurkan menggunakan referensi dari jurnal ilmiah nasional / internasional dari total seluruh referensi yang digunakan dan merupakan terbitan terbaru.

BAB 3. METODOLOGI PERANCANGAN

Berisi data-data pendukung untuk perancangan dan diagram alir atau fishbone diagram diikuti dengan penjelasan dibawahnya.

BAB 4. IMPLEMENTASI DAN PENGUJIAN

Berisi data-data penelitian yang dihasilkan dan analisa dari data-data tersebut. Data-data ditampilkan dalam bentuk diagram yang menarik, dan desain dengan software agar mudah dilakukan pembahasan dan analisa serta mudah dimengerti pembaca.

BAB 5. KESIMPULAN DAN SARAN

Berisi kesimpulan dari hasil penelitian penulis yang dituangkan dalam bentuk penomoran. Tidak dalam bentuk penjelasan/serta analisa data. Saran ditambahkan jika ada beberapa hal yang perlu ditambahkan berkaitan dengan kegiatan Tugas Akhir ini misalnya kendala dalam Tugas Akhir, penelitian lanjut yang diperlukan, dan sebagainya.

DAFTAR REFERENSI

LAMPIRAN