1 PENDAHULUAN

1.1 Latar Belakang

Badan Meteorologi, Klimatologi, dan Geofisika (BMKG) adalah Lembaga Pemerintah Non Departemen Indonesia. BMKG mempunyai tugas melaksanakan tugas pemerintahan di bidang Meteorologi, Klimatologi, Kualitas Udara dan Geofisika sesuai dengan ketentuan perundang-undangan yang berlaku. BMKG Wilayah II memiliki server yang berfungsi untuk menampung banyak informasi dan data yang penting, namun di sana belum terdapat sistem untuk mendeteksi serangan dari luar, hal tersebut mengakibatkan mudahnya serangan untuk masuk ke dalam jaringan internal atau tidak terdeteksinya aktivitas yang mencurigakan dalam jaringan internal, salah satu contoh yaitu serangan *flooding*.

Penelitian yang dilakukan oleh (Lanke & Jacob, 2014) menjelaskan bahwa teknik *flooding* merupakan serangan yang ditunjukkan untuk mengacaukan atau menghentikan sebuah layanan secara bersama-sama. Aktifitas *flooding* merupakan serangan terhadap sebuah komputer atau *server* di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Salah satu teknik yang digunakan untuk mendeteksi serangan *flooding* adalah penerapan *Intrusion Detection System* (IDS), seperti pada penelitian (Stiawan et al., 2012) yang menggunakan *Intrusion Detection System* (IDS) untuk mengidentifikasi adanya serangan dan dapat memberikan peringatan serangan yang terjadi pada *server*.

Selanjutnya pada penelitian (Indra, 2010) menyebutkan bahwa untuk mengurangi resiko pada celah gangguan keamanan pada jaringan *server* menggunakan *tool* Snort yang merupakan *Intrusion Detection System* (IDS) paling unggul dalam menganalisis lalu lintas jaringan dan *packet logging IP network* yaitu mencatat paket (informasi) yang melalui jaringan. Snort digunakan untuk mendeteksi ancaman seperti *buffer overflows*, yaitu sebuah kelemahan yang mudah untuk ditemukan dan dimanfaatkan oleh *hacker* dalam sebuah sistem, *port scanning* atau aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah mesin, nmap maupun *port scanner* lainnya. Snort memberikan informasi serangan berupa *alert log* yaitu catatan peringatan yang berisi informasi penting tentang pesan kesalahan dan pengecualian yang terjadi selama sistem berjalan. Pada tugas akhir ini diterapkan sistem *Intrusion Detection System* (IDS) Snort untuk mendeteksi serangan *flooding* pada *server*. *Intrusion Detection System* (IDS) adalah sebuah sistem untuk mendeteksi adanya serangan yang terjadi pada jaringan komputer seperti pencurian data, informasi dan perusakan sistem.

IDS dapat diimplementasikan pada aplikasi Suricata ataupun Snort. Snort merupakan IDS berbasis *Open Source* yang dirilis pada tahun 1998. Snort sendiri

merupakan IDS *singlethreading* yang menggunakan *rules* sebagai teks untuk mengisntruksi, menangani dan memberi aksi terhadap *event* yang terdeteksi. Snort sendiri sudah berkembang menjadi IDS dan IPS yang sangat teruji (White, 2013). Snort dioperasikan menggunakan *command lines* dan Berkeley Packet Filter (*optional*). *Rules* Snort sangat mudah diimplementasikan. Walaupun terbilang cukup mudah, rules Snort sendiri sangatlah ampuh untuk mendeteksi segala jenis paket yang mencurigakan (Kumar, 2014). Menurut Ashish Kumar dalam jurnalnya yang berjudul *Recent Advances in Intrusion Detection Systems: An Analytical Evacuation and Comparative Study*, disebutkan bahwa sebagai IDS, Snort memliki beberapa fitur yang bisa dimanfaatkan oleh penggunannya (Kumar, 2014). Berikut fitur yang ada di Snort adalah dapat berjalan pada semua jenis sistem operasi, *singlethread*, kemampuan dalam memeriksa *protocol*, kemampuan dalam memerika kondisi/*event*, kemampuan dalam mereassembly paket paket, menyediakan hasil output dalam bentuk ASCII, Tersedia versi GUI untuk hasil analisa.

Pada tahun 2009, US *Department of Homeland Security* memberikan dana hibah yang besar kepada sebuha organisasi yang baru terbentuk bernama Open *Information Security Foundation* (OISF). Hal ini bertujuan untuk dibuatnya IDS *multithreaded sebagai alternatif dari IDS Snort. IDS ini bernama Suricata. Pada* tahun 2010, Suricata meluncurkan IDS mereka untuk pertama kali dengan versinya yaitu 1.2. (White, 2013). Pengoperasian Suricata tidak terlalu berbeda dengan Snort, dapat dioperasikan dengan *command lines* dan juga *Berkeley Packet Filter*. *Rules* Suricata juga tidak jauh berbeda dengan Snort. Bahkan *rules* Snort dapat diimplementasikan ke dalam Suricata (White, 2013). Menurut Ashish Kumar dalam jurnalnya yang berjudul *Recent Advances in Intrusion Detection Systems: An Analytical Evacuation and Comparative Study*, disebutkan bahwa sebagai IDS, Suricata memliki beberapa fitur yang bisa dimanfaatkan oleh penggunannya (Kumar, 2014). Berikut merupakan fitur yang ada di Suricata yaitu, dapat berjalan pada semua jenis sistem operasi, *multithread*, tersedia fitur *Intrusion Prevention System* (IPS), kemampuan dalam memeriksa protokol, tersedia fitur *Network Security Monitoring* (NSM), kemampuan dalam memeriksa kondisi/*event*.

Pada tugas akhir ini IDS diimplementasikan pada aplikasi Snort. Pada konsep kerjanya IDS akan mencoba mendeteksi adanya tindakan ancaman yang ada dan segera mengirimkan informasi pada administrator jaringan. Sistem pengiriman informasi terhadap aktivitas mencurigakan yang ada saat ini umumnya dilakukan secara manual oleh administrator, hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator. Selain itu administrator harus selalu *standby* untuk melihat kondisi jaringan jika terjadi serangan.

Bot atau yang dikenal dengan robot merupakan solusi untuk menggantikan suatu aktivitas yang berulang dan dapat diandalkan untuk melakukan otomatisasi sebuah kegiatan, salah satu aplikasi yang menyediakan fitur bot adalah Telegram atau biasa disebut bot Telegram. Bot Telegram adalah sebuah bot atau robot yang diprogram dengan berbagai perintah untuk menjalankan serangkaian instruksi yang diberikan oleh pengguna. Bot ini hanyalah sebuah akun Telegram yang dioperasikan oleh perangkat lunak yang memiliki fitur AI. Fitur AI merupakan

kecerdasan buatan dapat diartikan sebagai teknologi komputer yang memiliki kecerdasan seperti manusia.

Telegram menyediakan fitur bot yang dapat memudahkan *user* untuk melakukan proses otomatisasi terhadap sebuah sistem, sehingga mengurangi campur tangan *user* di dalamnya. Telegram Bot sebagai media *alert* serangan yang terjadi. Implementasi Snort IDS pada Server menggunakan Notifikasi melalui Aplikasi Telegram dapat menyederhanakan proses *monitoring* dengan cara mengirimkan informasi secara otomatis setiap kali sistem mengalami serangan dari pihak luar.

1.2 Tujuan

Tujuan dari Implementasi Snort IDS pada Server dengan Notifikasi melalui Aplikasi Telegram di BMKG Wilayah II adalah:

1. Mendeteksi serangan awal, yaitu serangan yang bersifat mengecek keamanan dari suatu server, seperti DDOS, *Port Scanning*, dan serangan yang bersifat *attack* (mengganggu) seperti *flooding*.
2. Mencegah penyusup masuk ke jaringan *internal*.
3. Mengirimkan notifikasi serangan dini melalui aplikasi telegram.

1.3 Manfaat

Manfaat yang diperoleh dari tugas akhir ini yaitu meningkatkan keamanan jaringan pada server di BMKG Wilayah II dengan mengimplementasikan Snort IDS dan untuk memfasilitasi sistem pelaporan terhadap aktivitas mencurigakan dengan notifikasi melalui aplikasi telegram sehingga integritas sistem tidak bergantung pada ketersediaan dan kecepatan administrator selain itu administrator tidak harus selalu *standby* untuk melihat kondisi jaringannya jika terjadi penyusupan.

1.4 Ruang Lingkup

Ruang lingkup dari Impementasi Snort IDS pada Server dengan Notifikasi melalui Aplikasi Teglegram di BMKG Wilayah II adalah:

1. Implementasi menggunakan software Snort-2.9.15.1.
2. Implementasi menggunakan software Telegram.
3. Implementasi Snort IDS hanya di implementasikan pada VPS (*Virtual Private Server*).
4. Percobaan serangan hanya melakukan jenis serangan *flooding*.
5. Sistem akan berjalan jika terkoneksi dengan *internet*.