BAB 1
PENDAHULUAN

1.1 Latar Belakang Penelitian

Pada saat ini perkembangan zaman sudah memasuki era digitalisasi. Pada era digitalisasi ini banyak perusahaan atau instansi pemerintahan dari berbagai sektor sudah beranjak dari sistem konvensional atau manual menjadi menggunakan sistem. Dengan kemajuan yang ada ini tentunya banyak pihak berharap agar pelayanan dan kenyaman yang didapat oleh pelanggan atau rekan bisnis menjadi mudah dan cepat serta dapat dilakukan dimana saja dan kapan saja. Tentunya dengan demikian kegiatan bisnis atau industri dan bidang lainnya menjadi lebih berkembang. Pada era digital ini bisnis berkembang menjadi lebi pesat dan membuka banyak peluang bisnis dan usaha baru diberbagai sector, meningkatkan efisiensi operasional, serta mempercepat kemajuan bisnis (Widya Astuti dkk., 2023)

Perkembangan pada zaman digitalisasi ini tentunya perlu didukung dengan adanya infrastruktur yang mendukung didalamnya. Hal yang perlu disiapkan tentunya infrastruktur jaringan. Infrastruktur jaringan ini memiliki peran penting untuk menghubungkan sistem satu dengan sistem lainnya. Pada umumnya infrastruktur jaringan ini dibuat menyesuaikan kebutuhan pada instansi atau industri yang memerlukannya.

Jaringan Komputer merupakan sekumpulan sistem yang didalamnya terdiri dari beberapa komputer yang bisa saling berkomunikasi dan berbagi sumber daya antara komputer satu dengan komputer lainnya. Jaringan komputer sendiri terdiri dari keterhubungan antara perangkat keras (*Hardware*) dan juga perangkat lunak (*Software*). Jaringan komputer biasanya terdiri dari bagian yang menerima layanan dan juga mengirimkan layanan (*service*). Pihak yang menerima layanan biasa disebut dengan *client*, sedangkan pihak yang memberikan layanan kepada klien biasa disebut dengan *server* (Aprilyano Ekklesia Tangkowit dkk., 2021). Komputer *server* merupakan sebuah komputer dengan kemampuan spesifikasi yang lebih tinggi dibandingkan dengan komputer *client*. Dengan kemampuan yang dimilikinya komputer *server* bisa melayani beberapa komputer *client* yang terhubung ke komputer *server* tersebut. Semakin canggih komputer *server*nya maka semakin

Muhamad Hisyam Nugraha Solihin, 2024
IMPLEMENTASI APLIKASI SNORT PADA SISTEM KEAMANAN SERVER DENGAN NOTIFIKASI TELEGRAM
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

banyak pula komputer *client* yang bisa terhubung dengan layanan *service* nya. Seiring dengan banyaknya jumlah *client* yang terhubung dengan suatu *server* maka semakin besar juga ancaman yang akan diterima oleh *server* tersebut.

Setelah memiliki infrastruktur yang memadai untuk menunjang percepatan bisnis dan industri jaringan komputer yang berperan untuk menghubungkan sistem dan *client* didalamnya juga memiliki kerentanan. Kerentanan yang bisa mengancam pada jaringan komputer terutama *server* ini adalah ancaman serangan siber. Ancaman siber ini bukan hanya dilakukan dari Indonesia, namun ancaman ini hadir dari seluruh dunia. Di Indonesia sendiri sejak awal januari hingga maret 2024 terdapat sebanyak 6 juta lebih ancaman serangan siber, dan ada 5.862.955 serangan yang berhasil diblokir, jumlah itu turun dari tahun lalu yang berada disangka 7.651.841 pendeteksian (CNN Indonesia, 2024).

Ancaman siber yang dikirimkan oleh penyerang tentunya beragam dan banyak jenisnya. Tujuan dari serangan ini pun sangan beragam, namun biasanya serangan ini dilakukan bertujuan untuk menghabiskan sumberdaya pada *server* sehingga kemampuan *server* untuk memberikan layanan kepada *client* menurun atau bahkan maati. Dari serangan yang dihasilkan tentu akan menimbulkan kerugian bagi pihak korban. Serangan yang biasanya digunakan oleh penyerang untuk menghabiskan sumberdaya *server* biasanya menggunakan jenis serangan DDoS atau serangan lain yang bisa membuat kinerja *server* menjadi berlebihan.

Denial Distributed Of Service (DDoS) merupakan sebuah ancaman yang nyata bagi *server*. Serangan DDos ini bertujuan untuk melumpuhkan service yang sedang berjalan pada sebuah jaringan atau *server*, serangan ini berjalan dengan cara mengirimkan ribuan atau bahkan ratusan ribu *request* yang mana *request* ini merupakan permintaan palsu yang berasal dari *device* atau puluhan *device* palsu yang mana serangan ini akan mengakibatkan sistem layanan pada *server down* dan tidak dapat diakses (Ubaidillah dkk., 2023). Serangan DDoS ini pernah dialami oleh pemerintahan DKI Jakarta pada pertengahan maret 2020, liputan6 mengabarkan bahwa situs resmi pemantauan Covid-19 DKI Jakarta mengalami serangan DDoS yang mengakibatkan situs tidak bisa diakses (Damar, 2020). *Port scanning* merupakan jenis serangan siber yang juga sering dilancarkan oleh penyerang atau *hacker* kepada *server*, menurut definisinya *port scanning* adalah kegiatan *probe*

dalam jumlah yang besar dengan menggunakan *tool* secara otomatis, dalam hal ini adalah Nmap (Bayu Rendro dkk., 2020). tujuan dari serangan nmap ini adalah mencari nformasi yang diinginkan seperti port-port yang terbuka pada *server*, sistem operasi, dan versi sistem operasi dari *server* (Agus Eka Pratama & Mega Handayani, 2019).

Serangan siber ini juga pernah menyerang perbankan di Indonesia. Pada tanggal 16 Mei 2023 terjadi serangan terhadap Bank Syariah Indonesia yang disebab kan oleh *ransomeware LockBit* serangan ini menyebabkan 15 juta data nasabah dijual pada situs *dark web* (TEMPO, 2023). Dari pengalaman penulis yang kebetulan sedang melakukan magang pada Bank Rakyat Indonesia ditahun yang sama serangan yang mengarah pada *server* di instansi perbankan memang sangat sering terutama serangan pada lalu lintas jaringan agar *server down* dan nasabah tidak dapat mengakses layanan yang tersedia, pada pengalaman penullis tim dari masing-masing aplikasi akan membuat sistem monitoring *server* menggunakan *platform* UI Path, *platform* tersebut akan membuat sistem otomasi dan mengirimkan informasi mengenai kondisi *server* seperti pemakaian CPU, RAM, DISK secara berkala (biasanya setiap 30 menit) kepada anggota tim IT, sistem tersebut membantu tim dalam hal pemantauan *server* namun sering kali terabaikan, karena pesan yang dikirimkan adalah berupa *screenshoot* gambar dari kondisi CPU, RAM, DISK dari beberapa *server* sehinga Ketika terjadi serangan atau kenaikan penggunaan sumber daya secara tiba-tiba anggota tim sering kali tidak menyadari karena tidak ada *alert* yang menyatakan adanya serangan atau lalu lintas jaringan yang tidak normal, mereka hanya dikirimkan gambar saja yang tentunya ketika pekerjaan lain yang mereka lakukan membuat sedikit menurun kewaspadaanya.

Maraknya kejahatan siber yang terjadi pada saat ini tentunya perlu direspon dengan mingkatkan sistem pertahanan yang kuat untuk menahan dan mencegah serangan siber bisa menghambat jalannya komunikasi antar jaringan komputer. Sistem deteksi serangan siber merupakan sebuah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusupan serangan siber. Guna mencegah terjadinya serangan maka dibutuhkan sistem untuk memantau dan mendeteksi kegiatan mencurigakan pada jaringan *server*. Meningkatkan sistem keamanan pada *server* akan meningkatkan pertahanan dan

respons jika terjadi serangan siber (Shafiyyah dkk., 2024). Ada beberapa aplikasi yang bisa di gunakan yaitu snort dan suricata.

Pada jurnal yang berjudul "Model Pemantauan Keamanan Jaringan Melalui Aplikasi Telegram Dengan *Snort*" hasil yang didapatkan adalah sistem keamanan jaringan menggunakan snort ini menerapkan satu *rules* untuk mendeteksi apabila ada sistem yang melakukan ping kepada *server* dan sistem akan mengirimkan notifikasi kepada administrator jaringan sebagai tanda adanya serangan dari jaringan lain (Natanael Christianto & Wiwin Sulistyo, 2021), pada penelitian selanjutnya yang juga menggunakan sistem snort dan notifikasi telegram menggunakan 2 jenis serangan yaitu *NMAP Scanning* dan *SYN-Flood* pada serangan yang diuji kan snort berhasil mendeteksi serangan dan mengirimkan notifikasi kepada telegram (Desma Mahendra & Sisilia Mukti, 2022).

Deteksi tentunya perlu diawasi oleh seorang admin jaringan atau seseorang yang menjaga keamanan jaringan. Seorang admin jaringan ini harus siaga setiap saat karena serangan DDoS tidak dapat diprediksi kedatangannya. Sistem *Alert* bisa menjadi bahan pertimbangan sebagai sistem *back up* apabila admin jaringan sedang kurang teliti dalam mengawasi lalu lintas jaringan yang diawasinya.

Sistem *Alert* ini bisa dibuat dengan memanfaatkan bot pada telegram. Telegram merupakan sebuah aplikasi pesan instan multi*platform* yang berbasis *cloud* dan bersifat gratis. Telegram bot merupakan fitur yang ditawarkan oleh telegram dan mempunyai fungsi khusus serta berjalan otomatis sesuai dengan perintah penggunanya.

Aplikasi telegram dipilih sebagai kanal yang digunakan untuk mengirimkan dan menerima hasil laporan dari snort karena menurut penelitian Sahrul dan Wibawa (2021) mengatakan bahwa telegram memiliki keunggulan dimana API yang digunakan merupakan API terbuka sehingga dapat digunakan tanpa perlu aplikasi pihak ke tiga selain itu pengiriman file bisa hingga 1.5 gb sehingga cocok untuk di gunakan sebagai *platform* penerima notifikasi serangan dari snort (Shahrul & Wibawa, 2021).

1.2 Rumusan Masalah

Berdasarkan permasalahan yang sudah dijelaskan sebelumnya, peneliti merumuskan beberapa rumusan masalah pada penelitian ini diantaranya:

1. Bagaimana implementasi snort sebagai sistem keamanan *server* dengan notifikasi melalui bot telegram?
2. Bagaimana performa snort dalam pendeteksian serangan siber untuk sistem keamanan *server*?
3. Bagaimana tingkat keberhasilan telegram sebagai media penerima notifikasi menerima peringatan serangan yang terdeteksi oleh snort?

1.3 Batasan Masalah

Perancangan Implementasi aplikasi Snort pada sistem keamanan *server* dengan notifikasi telegram memiliki beberapa Batasan masalah dalam proses perancangannya yaitu

1. Perangkat *server* menggunakan virtual box (ubuntu *server*).
2. Sistem snort digunakan untuk mendeteksi jenis serangan *Slow http*, POP3, *Port Scanning*, DDoS, SNMP, ICMP, *SQL Injection, XSS, IP Spoofing*.
3. Serangan dikirimkan menggunakan kali linux

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dari penelitian ini untuk:

1. Membuat sistem keamanan *server* menggunakan snort dan telegram
2. Mengintegrasikan snort dengan telegram untuk mempercepat respon terhadap serangan.
3. Mengetahui performa pendeteksian snort terhadap serangan siber.

1.5 Manfaat Penelitian

Berdasarkan hasil pemaparan tujuan penelitian yang telah dipaparkan sebelumnya, manfaat utama dari penelitian yang penulis buat ini adalah untuk meningkatkan keamanan jaringan terutama keamanan *server* melaluli implementasi aplikasi snort dan dikombinasikan dengan notifikasi pada telegram jika ada serangan yang terdeteksi oleh snort. Penelitian ini bisa dijadikan kajian dan dasar pengembangan sistem keamanan yang dipadukan dengan *platform* lain untuk meningkatkan performa penanganan serangan siber pada bidang IT mengingat banyaknya kasus serangan siber yang terjadi. Manfaat yang bidang diambil sebagai berikut:

1.5.1 Manfaat Teoritis

Manfaat teoritis yang diharapkan adalah sebagai berikut:

A. Memberikan inovasi teknologi dalam bidang keamanan siber dalam penelitian implementasi snort pada jaringan *server* apabila terjadi anomali jaringan sebagai indikasi awal terjadinya serangan siber yang dipadukan dengan integrasi pesan *alert* yang akan terkirim menggunakan bot telegram.
B. Memberikan referensi bagi penelitian selanjutnya agar pengembangan sistem keamanan jaringan bisa lebih baik lagi kedepannya.
C. Memberikan literatur akademis di bidang keamanan jaringan dengan memberikan informasi mengenai hasil penelitian implementasi aplikasi snort dan notifikasi telegram.

1.5.2 Manfaat Praktis

A. Bagi beberapa perusahaan terutama perusahaan yang bergerak dalam bidang penyedia layanan penyewaan *server* atau data center dan instansi perbankan tentunya sistem ini bisa diterapkan guna membantu kinerja tim network administrator pada perusahaan-perusahaan tersebut dalam melakukan pencegahan terjadinya serangan siber pada *server* di perusahaan mereka.
B. Dengan adanya fitur *alert* yang dikirimkan oleh bot telegram kepada pengguna tim network security bisa lebih cepat dan tanggap apabila terjadi serangan mendadak pada wkatu yang kurang pengawasannya.
C. Dengan meningkatnya keamanan *server* diharapkan bisa membantu mengurangi dampak dari serangan siber yang terjadi terutama dampak ekonomi yang sangat terasa bila suatu instansi atau perusaan mengalami serangan siber.

1.6 Struktur Organisasi Skripsi

Pada penelitian yang dilakukan ini dibagi kepada beberapa bagian yang sesuai dengan pedoman KTI UPI 2021, berikut beberapa bagian yang dilakukan:

1. PENDAHULUAN

Pada bagian bab I ini berisikan mengenai uraian dari latar belakang pemilihan topik penelitian yang penulis angkat lalu rumusan masalah penelitian yang dilakukan, tujuan dari penelitian, manfaat teoritis dan prkatis dari penelitian, batasan masalah, dan struktur organisasi skripsi.

2. KAJIAN PUSTAKA

Pada bab II Kajian Pustaka ini membahas mengenai studi litelatur terkait penelitian. Beberapa bagian bab ini menjelaskan tentang konsep, metode, teori, dan teknologi yang digunakan.

3. METODE PENELITIAN

Pada Bab III Metode Penelitian membahas mengenai prosedur penelitian. Pada bab ini mencakup metode penelitian, metode pengujian dan metode analisis data.

4. TEMUAN DAN PEMBAHASAN

Pada Bab IV ini berisikan Temuan dan Pembahasan akan memaparkan hasil yang diperoleh dari penelitian yang telah penulis lakukan, berupa hasil perancangan perancangan dan implementasi snort. Hasil integrasi snort dengan telegram dan hasil pemblokiran ip yang dilakukan oleh skrip.

5. SIMPULAN, IMPLIKASI DAN REKOMENDASI

Pada Bab V simpulan, implikasi dan rekomendasi berisi tentang kesimpulan yang diperoleh berdasarkan hasil penelitian yang telah penulis lakukan, dan membahas mengenai saran terkait rencana pengembangan kedepannya berdasarkan hasil penelitian yang didapatkan.