BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan meningkatnya penggunaan jaringan dan internet, peningkatan juga terjadi pada perkembangan serangan keamanan jaringan. Oleh karena itu, penting untuk secara efektif melindungi *webserver* dari berbagai jenis potensi serangan, upaya penyusupan, dan pemindaian yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Dalam upaya menjaga *network security*, diterapkan suatu konsep dasar yang dikenal sebagai CIA *Triad*, yang melibatkan tiga aspek utama. Sebagai langkah pertama, terdapat suatu elemen kunci bernama kerahasiaan (*Confidentiality*), yang memfokuskan pada pembatasan akses terhadap informasi penting. Sebagai langkah kedua, integritas (*Integrity*) menjadi elemen yang memegang tanggung jawab utama untuk menjamin keutuhan dan ketepatan informasi. Terakhir, tetapi tidak kalah penting, ketersediaan (*Availability*) menjadi komponen yang menjamin informasi selalu tersedia saat dibutuhkan dan hanya dapat diakses oleh pihak yang berwenang [1].

Dalam laporan dari perusahaan internet *security* "Kaspersky Lab," tercatat adanya peningkatan yang signifikan dalam serangan *Bruteforce* secara global. Pada Februari 2020, angka serangannya mencapai 93,1 juta, namun meningkat pesat menjadi 409 juta pada November 2020. Tak ketinggalan, Indonesia juga mencatat 12,8 juta serangan *Bruteforce* pada Februari 2021. Serangan *Bruteforce* merupakan metode di mana para pelaku mencoba semua kombinasi kemungkinan *username* dan *password* untuk memperoleh akses ke server. Di sisi lain, laporan keamanan aplikasi Veracode mengungkapkan bahwa sekitar 32% dari aplikasi *web* mengalami kerentanan SQL *Injection*. Selain itu, Badan Siber dan Sandi Negara (BSSN) juga melaporkan bahwa sebanyak 73% laporan kerentanan yang diterima melalui *Voluntary Vulnerability Disclosure Program* (VVDP) pada periode Januari hingga April 2019 berhubungan dengan kerentanan SQL *Injection*. Dimana serangan SQL ditujukan pada *webserver* dengan menggunakan kode SQL untuk mencuri, menghapus, atau mengubah data yang ada pada *database*. Namun, bukan hanya itu, pada kuartal pertama tahun 2023, perusahaan keamanan siber Cloudfare dari

Amerika Serikat juga mencatat rekor serangan DoS terbesar yang pernah terjadi di dunia, mencapai 71 juta permintaan per detik dengan targetnya acara NFL Super Bowl 2023. Serangan DoS tersebut mengirimkan banyak permintaan ke sumber daya server yang diserang, bertujuan untuk membebani kapasitas server sehingga server tidak dapat menangani jumlah permintaan yang tinggi, yang pada akhirnya menghambat akses oleh pengguna yang sah ke *webserver* [2][3][4].

Gangguan signifikan terhadap kelancaran operasi resource server yang muncul akibat serangkaian insiden, memperlihatkan perlunya penelitian yang mampu merefleksikan keadaan yang sedang dihadapi. Oleh karena itu, landasan penelitian ini diperkuat oleh parameter-parameter yang telah terbukti efektif berdasarkan penelitian-penelitian sebelumnya. Salah satunya adalah karya yang telah dijalankan oleh Daryyl Santoso dan timnya, berjudul "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS". Meski parameter CPU usage yang diaplikasikan dalam penelitian tersebut telah terbukti cocok sebagai indikator, namun terdapat kelemahan dalam kedalaman presentasi rincian hasil penelitian tersebut. Walau pemantauan penggunaan CPU menjadi unsur kunci, namun data spesifik terkait penggunaan CPU tidak dihadirkan dalam bentuk numerik yang memberikan kesimpulan yang pasti. Dengan demikian, dapat disimpulkan bahwa pendekatan yang digunakan dalam riset tersebut cenderung lebih condong pada metode penelitian kualitatif daripada kuantitatif [5].

Dalam mengkaji kembali penelitian sebelumnya yang diarahkan oleh Faula Tanang Anugrah dan timnya dalam riset berjudul "Implementasi *Intrusion Prevention System* (IPS) Menggunakan Suricata Untuk Serangan SQL *Injection*", dilakukan penggunaan parameter *response time* sebagai ukuran kinerja *webserver* yang dihadirkan kepada pengguna. Namun, dalam analisis yang lebih mendalam, terdapat beberapa kelemahan yang patut diperhatikan. Salah satu aspek yang mencuat adalah nilai *response time* rata-rata sebesar 4.2 ms. Meskipun angka ini mungkin terlihat rendah, perlu diakui bahwa dampak dari keterlambatan semacam itu dapat mempengaruhi penyajian konten *web* kepada pengguna akhir, meskipun hanya dalam skala ringan [6].

Penggunaan Telegram *bot* pada perangkat smartphone juga berguna dalam mengelola jaringan dan mengurangi risiko. *Bot* ini dikonfigurasi untuk mengirimkan pemberitahuan instan kepada *administrator*, khususnya saat terjadi peningkatan resource yang berlebihan, sehingga *administrator* dapat segera menindaklanjuti apakah itu merupakan serangan jaringan atau tidak [7].

Dengan mempertimbangkan beberapa kelemahan yang teridentifikasi dalam riset sebelumnya, maka dilakukan sebuah penelitian dengan judul "Implementasi *Intrusion Prevention System* (IPS) Sebagai Sistem Keamanan Jaringan Dari Serangan *Bruteforce*, SQL *Injection* Dan DoS Dengan Notifikasi Telegram". Harapannya, penulis dapat memberikan yang berarti dalam ranah keamanan jaringan dengan mengidentifikasi serta menghalau upaya serangan *Bruteforce*, SQL *Injection* dan Denial of Service (DoS) menggunakan kombinasi *Intrusion Prevention System* (IPS) dan dukungan Telegram *bot* berdasarkan keefektifan *rules* yang diukur melalui tanggapan penggunaan CPU dan *memory* disertai dengan kinerja waktu respons server yang ditujukan bagi para *normal user*.

1.2 Rumusan Masalah

Dalam konteks yang telah dijelaskan sebelumnya, penelitian ini mengajukan rumusan masalah berikut:

1. Bagaimana merancang sistem keamanan jaringan yang mampu secara efektif mengatasi serangan jaringan tipe *Bruteforce*, SQL *Injection*, dan DoS?
2. Bagaimana menganalisis *rules Intrusion Prevention System* (IPS) agar efektif dalam mendeteksi dan mencegah ancaman *Bruteforce*, SQL *Injection*, dan DoS?
3. Bagaimana kinerja *webserver* dengan diterapkannya *Intrusion Prevention System* (IPS) yang dievaluasi berdasarkan parameter penggunaan CPU dan *memory*, serta *response time* yang dihasilkan oleh *webserver* kepada klien?
4. Bagaimana pemanfaatan Telegram *bot* untuk mengirimkan pemberitahuan kepada *administrator* jaringan ketika terdeteksi adanya ancaman serangan?

1.3 Batasan Masalah

Untuk menjaga fokus dan mengarahkan pada inti permasalahan, berikut adalah beberapa batasan masalah yang diidentifikasi dalam penelitian ini:

1. Memanfaatkan Suricata sebagai alat *Intrusion Prevention System* (IPS).
2. Menggunakan *platform* DVWA sebagai *webserver*.
3. Pengujian dilakukan menggunakan tiga jenis serangan, yaitu HTTP *Bruteforce*, SQL *Injection*, dan DoS dengan ICMP *flood*.
4. Penelitian ini dilakukan pada *Local Area Network* dengan topologi *star*.
5. Sistem operasi yang digunakan oleh *attacker*, *webserver*, dan *normal user* adalah Linux Ubuntu 22.04 LTS.
6. *Tool*s Hydra, SQLMap, dan Hping3 digunakan untuk melakukan uji coba penyerangan.
7. Parameter yang diamati dalam penelitian ini mencakup *response time*, penggunaan CPU, dan *memory*.
8. Pengumpulan data menggunakan *log* Suricata dan notifikasi server melalui Telegram *bot* menggunakan bahasa pemrograman Python.

1.4 Tujuan Penelitian

Di bawah ini adalah beberapa tujuan yang ingin dicapai oleh penulis dalam penelitian ini.:

1. Merancang sebuah sistem keamanan jaringan dengan menerapkan metode IPS Suricata dilengkapi dengan Telegram *bot* sebagai *monitoring*.
2. Menganalisis penerapan *rules* Suricata yang efektif dalam menghadapi ancaman *Bruteforce*, SQL *Injection* dan DoS berdasarkan CPU dan *memory usage* beserta *response time*.

1.5 Manfaat Penelitian

Setelah penelitian ini selesai dilakukan, diharapkan dapat memberikan berbagai manfaat yang signifikan. Pertama, melalui peningkatan tingkat keamanan jaringan terhadap serangan *Bruteforce*, SQL *Injection*, dan DoS, perusahaan dapat memperoleh kepercayaan lebih dari pelanggan terhadap layanan dan produk yang mereka tawarkan. Ini berarti bahwa pelanggan akan merasa lebih aman dan nyaman

dalam menggunakan layanan perusahaan, yang pada gilirannya dapat meningkatkan loyalitas pelanggan.

Kedua, dengan mengurangi serangan yang masuk dan meningkatkan pemantauan *realtime*, perusahaan dapat mengurangi risiko *downtime* atau gangguan layanan. Dengan kata lain, peningkatan keamanan ini akan menghasilkan layanan yang lebih stabil dan konsisten untuk pelanggan. Hal ini tentunya akan meningkatkan kepuasan pelanggan dan menjaga reputasi perusahaan.

Ketiga, penelitian ini juga dapat mencegah penyalahgunaan data pada server oleh pihak yang tidak bertanggung jawab. Ini sangat penting dalam menjaga kerahasiaan dan integritas data pelanggan dan perusahaan. Dengan demikian, perusahaan dapat mematuhi regulasi data yang berlaku dan menjaga kepercayaan pelanggan dalam mengelola data mereka.

Keempat, penelitian ini akan memberikan dukungan bagi *administrator* jaringan untuk melakukan pemantauan server secara *realtime* ketika terjadi serangan. Hal ini akan memudahkan pengambilan langkah-langkah keamanan jaringan selanjutnya. Dengan memiliki akses dan informasi yang lebih baik tentang serangan yang terjadi, *administrator* dapat merespons lebih cepat dan lebih efektif untuk melindungi jaringan perusahaan.

1.6 Sistematika Penulisan

Sistematika penulisan penelitian ini disusun dalam beberapa bab yang mengelompokkan ide utama sebagai berikut:

BAB I PENDAHULUAN

Bagian awal ini mengulas tentang latar belakang penelitian, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini berisi tinjauan pustaka yang menjadi referensi penulis dalam penyusunan penelitian, termasuk pembahasan tentang *Intrusion Prevention System* (IPS), *Firewall*, serangan *Bruteforce*, SQL *Injection*, *Denial of Service* (DoS), Suricata,

Hydra, SQLMap, Hping3, Telegram *bot*, dan topik terkait lainnya.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan, alur penelitian, alat yang digunakan, proses konfigurasi sistem *webserver*, *rule* yang digunakan IPS, konfigurasi *software* penyerang dan skema pengujian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan dan analisis dari hasil pengujian serangan keamanan jaringan dengan menitikberatkan pada target, baik sebelum maupun sesudah menggunakan metode *Intrusion Prevention System* (IPS) dengan memperhatikan parameter CPU, penggunaan *memory*, dan waktu *respons*.

BAB V PENUTUP

Pada bab ini, terdapat rangkuman dari analisis yang telah diuraikan pada bab sebelumnya, serta saran untuk pengembangan penelitian mendatang.