

BAB I PENDAHULUAN

1.1 Latar Belakang

Di era transformasi digital yang berkembang pesat, keamanan jaringan telah menjadi aspek yang sangat penting dalam menjaga keberlangsungan serta integritas operasional suatu organisasi [1]. Infrastruktur jaringan berbasis *cloud* memiliki tingkat kerentanan yang tinggi terhadap berbagai ancaman siber seperti *brute force* dan *Distributed Denial of Service (DDoS)*, sehingga diperlukan mekanisme perlindungan yang tidak hanya mampu mendeteksi, tetapi juga secara aktif merespons serangan [1].

Salah satu bagian yang memiliki peran vital dalam sistem keamanan jaringan adalah *gateway*, yaitu titik penghubung antara jaringan internal dengan jaringan eksternal [2]. Pada bagian ini, *firewall* berfungsi sebagai mekanisme pertahanan awal yang mengatur serta memfilter lalu lintas data yang keluar dan masuk ke dalam jaringan [2]. Penerapan mekanisme keamanan seperti *Web Application Firewall (WAF)* terbukti mampu meningkatkan perlindungan terhadap serangan siber [2].

pfSense merupakan salah satu solusi *firewall* berbasis *open-source* yang banyak digunakan dalam implementasi keamanan jaringan karena kemampuannya dalam mendukung berbagai fitur proteksi [3]. Integrasi *pfSense* dengan sistem deteksi seperti *Suricata* terbukti mampu mendeteksi dan mencegah berbagai jenis serangan, termasuk *brute force* [3]. Meskipun demikian, peran strategisnya sebagai pelindung utama jaringan menjadikan *pfSense* sebagai target yang rentan terhadap serangan siber [3]. Salah satu bagian yang sering menjadi sasaran adalah antarmuka manajemen berbasis web atau *Web Graphical User Interface (Web GUI)* yang digunakan oleh administrator untuk melakukan konfigurasi sistem [3]. Jika akses terhadap antarmuka ini berhasil dikuasai oleh pihak yang

tidak berwenang, maka potensi kompromi terhadap seluruh sistem jaringan menjadi sangat besar [3].

Salah satu bentuk serangan yang umum terjadi adalah serangan *brute force*, yaitu teknik yang dilakukan dengan mencoba berbagai kombinasi kredensial secara berulang hingga ditemukan pasangan *username* dan *password* yang valid [1]. Serangan ini biasanya menargetkan layanan autentikasi, termasuk halaman *login Web GUI* pada pfSense [3]. Permasalahan yang dihadapi adalah bahwa sistem bawaan pfSense cenderung hanya melakukan pencatatan aktivitas *login* tanpa memberikan respons otomatis terhadap upaya serangan tersebut [3]. Akibatnya, administrator harus melakukan pemantauan *log* secara manual untuk mendeteksi adanya aktivitas mencurigakan [3]. Proses ini tidak hanya kurang efisien, tetapi juga berpotensi menimbulkan keterlambatan dalam penanganan serta meningkatkan risiko kesalahan manusia [1].

Untuk mengatasi keterbatasan tersebut, diperlukan pendekatan yang lebih proaktif dalam mendeteksi dan menangani ancaman keamanan jaringan [1]. Berbagai solusi seperti *Intrusion Detection System (IDS)*, *Intrusion Prevention System (IPS)*, dan pemantauan *log* secara manual dapat digunakan, namun masih memiliki kelemahan, seperti tidak terpusat, terbatasnya kemampuan korelasi antar *log*, serta minimnya otomatisasi dalam merespons insiden keamanan [4].

Salah satu pendekatan yang lebih komprehensif adalah penggunaan sistem *Security Information and Event Management (SIEM)* yang mampu mengintegrasikan berbagai sumber *log* dalam satu platform terpusat serta melakukan analisis secara *real-time* [5]. Implementasi Wazuh sebagai SIEM terbukti dapat meningkatkan efektivitas pengelolaan *log* serta mempermudah proses analisis dan visualisasi insiden keamanan [5]. Selain itu, pengembangan Wazuh yang mengadopsi teknologi kecerdasan buatan

menunjukkan potensi dalam meningkatkan kemampuan otomatisasi respons terhadap ancaman secara lebih adaptif [6].

Dalam penelitian ini, sistem SIEM Wazuh diintegrasikan dengan *firewall* pfSense sebagai sumber utama *log*. pfSense dikonfigurasi untuk mengirimkan *log* melalui protokol *syslog* ke *server* Wazuh yang berada pada lingkungan *cloud*, sehingga proses analisis dapat dilakukan secara terpusat dan *real-time* [5].

Dalam penelitian ini, digunakan pendekatan arsitektur *Hybrid Cloud* dengan memanfaatkan *Cloud Virtual Private Server* (VPS) sebagai pusat pengolahan data *log*. Pendekatan ini bertujuan untuk mengurangi beban pemrosesan pada perangkat lokal sekaligus meningkatkan kemampuan sistem dalam menangani volume data yang besar [1].

Penelitian ini berfokus pada penerapan fitur *Active Response* pada Wazuh untuk mendeteksi dan memitigasi serangan *brute force* secara otomatis. Ketika aktivitas serangan teridentifikasi, sistem akan melakukan tindakan mitigasi berupa pemblokiran alamat IP penyerang melalui *firewall* pfSense [3]. Dengan mekanisme ini, serangan dapat dihentikan lebih cepat sebelum berdampak pada sistem internal jaringan [4].

Berdasarkan uraian tersebut, penelitian dengan judul "Implementasi *Active Response* pada SIEM Wazuh untuk Mitigasi Serangan *Brute Force* pada *Firewall* pfSense Berbasis *Cloud VPS*" dilakukan sebagai upaya untuk meningkatkan efektivitas sistem keamanan jaringan yang adaptif, terintegrasi, dan responsif terhadap berbagai ancaman siber.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara mengintegrasikan **SIEM Wazuh** pada *Cloud VPS* dengan **pfSense** di jaringan lokal melalui arsitektur *Hybrid Cloud* untuk memantau aktivitas log secara terpusat?
2. Bagaimana mengonfigurasi fitur *Active Response* pada Wazuh Manager agar dapat mendeteksi dan merespon serangan *brute force* pada halaman *Web GUI pfSense* secara otomatis?
3. Seberapa efektif penggunaan sistem *Active Response* dalam memitigasi serangan *brute force* dilihat dari parameter **kecepatan waktu respon** dan **akurasi pemblokiran alamat IP penyerang**?
4. Bagaimana stabilitas performa *Cloud VPS* dengan **RAM 4GB** dalam menjalankan fungsi manajer SIEM saat menangani *traffic log* dan eksekusi mitigasi dari infrastruktur lokal?

1.3 Batasan Masalah

Agar penelitian tetap terfokus pada tujuan yang telah ditetapkan, maka peneliti menetapkan batasan masalah sebagai berikut:

1. Perangkat lunak SIEM yang digunakan adalah Wazuh.
2. Sistem operasi pada *Cloud VPS* menggunakan **Ubuntu Server** dengan alokasi memori sebesar **4GB RAM**.
3. Target serangan difokuskan pada *Web GUI pfSense* melalui protokol *HTTP/HTTPS*.
4. Jenis serangan yang disimulasikan terbatas pada serangan *brute force* (kegagalan autentikasi berulang).

5. Metode mitigasi yang digunakan adalah *firewall-drop*, yaitu pemutusan koneksi IP penyerang pada tabel *firewall* pfSense melalui instruksi dari Wazuh Manager.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitian ini adalah sebagai berikut:

1. Membangun integrasi keamanan berbasis arsitektur *Hybrid Cloud* antara **Wazuh Manager** di *Cloud VPS* dan **pfSense** di jaringan lokal untuk memusatkan pemantauan *log* keamanan.
2. Mengimplementasikan fitur *Active Response* yang mampu mengotomatisasi proses mitigasi terhadap upaya akses ilegal melalui serangan *brute force* pada *Web GUI pfSense*.
3. Menganalisis performa sistem dalam hal **kecepatan waktu respon** mitigasi sejak serangan terdeteksi hingga alamat IP penyerang berhasil diblokir.
4. Membuktikan efektivitas dan stabilitas penggunaan **Cloud VPS dengan spesifikasi RAM 4GB** dalam menjalankan fungsi SIEM berskala menengah untuk kebutuhan pengamanan *gateway*.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dapat diperoleh dari hasil penelitian ini adalah sebagai berikut:

1.5.1 Manfaat Teoritis

- **Pengembangan Konsep SIEM:** Menjadi referensi dalam penerapan teknologi *Security Information and Event Management* (SIEM) berbasis *open-source* (Wazuh) yang dikombinasikan dengan arsitektur *Hybrid Cloud*.

- **Studi Mitigasi Otomatis:** Memberikan literatur tambahan mengenai efektivitas fitur *Active Response* dalam merespon anomali trafik secara *real-time* tanpa intervensi manusia.
- **Optimallsasi Sumber Daya:** Menjadi bahan kajian mengenai performa SIEM pada infrastruktur *cloud* dengan spesifikasi perangkat keras terbatas (RAM 4GB) namun tetap memiliki reliabilitas yang tinggi.

1.5.2 Manfaat Praktis

- **Bagi Administrator Jaringan:** Membantu mempermudah tugas pengawasan keamanan melalui sistem pemantauan terpusat dan otomasi mitigasi, sehingga mengurangi risiko *human error* dan keterlambatan respon terhadap insiden siber.
- **Bagi Instansi/Organisasi:** Memberikan solusi alternatif sistem keamanan yang handal namun ekonomis karena menggunakan teknologi *open-source*, guna melindungi aset digital dan kontrol panel utama (*Web GUI*) dari ancaman akses ilegal.
- **Bagi Praktisi IT:** Menyediakan panduan teknis atau *best practice* dalam melakukan integrasi antara *firewall* pfSense dengan manajer SIEM di lingkungan luar jaringan (*remote/cloud*).

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun secara sistematis untuk memberikan gambaran garis besar isi dari setiap bab sebagai berikut:

BAB I: PENDAHULUAN Bab ini menguraikan mengenai latar belakang masalah terkait ancaman serangan *brute force* dan pentingnya mitigasi otomatis. Selain itu, bab ini memuat rumusan masalah, batasan masalah agar penelitian tetap fokus, tujuan yang ingin dicapai, serta manfaat penelitian baik secara teoritis maupun praktis.

BAB II: TINJAUAN PUSTAKA Bab ini berisi tinjauan pustaka dari penelitian terdahulu yang relevan serta landasan teori yang digunakan sebagai dasar penelitian. Materi yang dibahas meliputi arsitektur SIEM Wazuh, fungsi *firewall* pfSense, konsep jaringan *hybrid cloud*, serta teori mengenai serangan *brute force* dan mekanisme *Active Response*.

BAB III: METODE PENELITIAN Bab ini mendeskripsikan metodologi yang digunakan peneliti dalam menyelesaikan masalah, mulai dari perancangan topologi jaringan yang menghubungkan jaringan lokal dan *Cloud VPS*, analisis kebutuhan sistem, hingga perancangan skenario pengujian serangan. Di dalamnya juga dijelaskan mengenai alat dan bahan yang digunakan dalam lingkungan *virtual*.

BAB IV: HASIL DAN PEMBAHASAN Bab ini merupakan inti dari penelitian yang memaparkan tahapan implementasi sistem, mulai dari instalasi dan konfigurasi hingga integrasi antar perangkat. Peneliti juga menyajikan hasil pengujian simulasi serangan *brute force*, analisis terhadap peringatan keamanan yang muncul, serta pembuktian efektivitas fitur *Active Response* dalam memblokir IP penyerang.

BAB V: PENUTUP Bab ini berisi kesimpulan yang ditarik peneliti dari hasil pengujian dan pembahasan untuk menjawab rumusan masalah yang telah diajukan. Selain itu, bab ini memuat saran-saran dari peneliti yang ditujukan untuk pengembangan penelitian selanjutnya di masa mendatang.