BAB II
KAJIAN LITERATUR

2. 1 Landasan Teori

Pada bab ini akan menjelasakan terkait teori dasar dan penelitian terkait yang digunakan penulis sebagai acuan dalam penyusunan penelitian.

2.1.1 Aplikasi Web

Aplikasi web merupakan sebuah aplikasi yang akan digunakan pada web browser manapun dan sistem operasi apapun, aplikasi web juga dapat dijalankan menggunakan internet maupun intranet [3]. Untuk saat ini aplikasi web digunakan dalam banyak sektor, mulai dari berjualan, sarana pembelajaran, sarana sosial seperti pengumpulan donasi, dan masih banyak lagi. Karena sebagian besar aplikasi web bergantung pada internet, perlu juga dimonitoring dan dijaga pada sisi keamanannya dengan itu diharapkan agar data dari pemilik dan pengguna aplikasi web menjadi aman, selain itu dengan adanya aktivitas monitoring dan analisa maka menjadi tau sisi mana yang sering diserang dan juga sisi mana yang perlu ditingkatkan lagi keamanannya.

2.1.1.1 Sejarah aplikasi web

Aplikasi web, juga dikenal sebagai aplikasi web, adalah aplikasi yang diakses melalui browser web yang berjalan di server web. Sejarah aplikasi web dimulai pada tahun 1990-an ketika internet semakin meluas dan internet semakin mudah digunakan. Pada awalnya, aplikasi web hanyalah halaman statis yang menampilkan teks dan gambar. Namun, seiring kemajuan teknologi, aplikasi web mulai menampilkan animasi, video, dan audio. JavaScript, bahasa pemrograman untuk aplikasi web, dirilis pada tahun 1995 dan semakin populer. Pada tahun 2000-an, aplikasi web mulai berkembang pesat, terutama dengan munculnya teknologi AJAX (Asynchronous JavaScript and XML). Teknik ini memungkinkan aplikasi web untuk meminta dan memperbaharui

data secara tidak serentak tanpa melakukan refresh halaman. Ini membuat aplikasi web lebih responsif dan lebih cepat.

Kemudian, pada tahun 2010-an muncul tren untuk mengembangkan aplikasi web dengan arsitektur berbasis API (*Application Programming Interface*) yang memungkinkan aplikasi web terhubung ke berbagai layanan dan platform lain, termasuk aplikasi mobile. Saat ini, aplikasi web semakin berkembang dengan diperkenalkannya teknologi terbaru seperti *Progressive Web App* (PWA), WebAssembly dan WebVR, yang memungkinkan pengembangan aplikasi web yang lebih kompleks dan interaktif. Aplikasi web juga semakin populer karena dapat digunakan di berbagai perangkat, termasuk komputer, tablet, dan ponsel cerdas, tanpa menginstal aplikasi.

2.1.1.2 Keamanan aplikasi web

Keamanan aplikasi web merujuk pada serangkaian praktik dan teknologi yang dirancang untuk melindungi aplikasi web dari ancaman keamanan seperti serangan peretas atau malware. Secara umum, keamanan aplikasi web terdiri dari tiga aspek: kerahasiaan, integritas, dan ketersediaan.

1. Kerahasiaan: Aspek kerahasiaan dalam keamanan aplikasi web menjamin bahwa informasi yang terkait dengan aplikasi, seperti data pengguna dan informasi rahasia lainnya, hanya dapat diakses oleh orang-orang yang diizinkan. Hal ini dapat dicapai melalui praktik keamanan seperti enkripsi data, autentikasi pengguna, dan otorisasi akses.
2. Integritas: Aspek integritas dalam keamanan aplikasi web memastikan bahwa data dan informasi yang dikirim melalui aplikasi web tidak dimanipulasi oleh pihak yang tidak berwenang. Hal ini dapat dicapai melalui teknologi seperti kontrol akses, enkripsi data, dan validasi input.
3. Ketersediaan: Aspek ketersediaan dalam keamanan aplikasi web menjamin bahwa aplikasi web selalu tersedia dan dapat diakses oleh pengguna yang sah. Hal ini dapat dicapai melalui teknologi seperti pengelolaan kapasitas, cadangan data, dan manajemen kesalahan.

Selain ketiga aspek utama di atas, keamanan aplikasi web juga dapat mencakup praktik keamanan tambahan seperti:

- Pemantauan dan pengawasan sistem: Melacak aktivitas aplikasi web dan sistem terkait untuk mendeteksi ancaman dan serangan peretas.
- Pembaruan keamanan: Memastikan bahwa aplikasi web selalu diperbarui dengan perangkat lunak terbaru dan patch keamanan untuk menghindari kerentanan keamanan yang dikenal.
- Pendidikan dan pelatihan pengguna: Mengedukasi pengguna tentang praktik keamanan internet dan bagaimana menghindari serangan phishing dan malware.

Secara keseluruhan, keamanan aplikasi web merupakan hal yang sangat penting untuk melindungi data dan informasi pengguna dari ancaman keamanan. Dengan menerapkan praktik dan teknologi keamanan yang tepat, pengembang aplikasi web dapat memastikan bahwa aplikasi mereka aman dan dapat diandalkan bagi pengguna yang mempercayainya.

2.1.1.3 Kerentanan aplikasi web

Kerentanan *website* (*website* vulnerability) adalah kelemahan atau celah dalam suatu situs web yang dapat dimanfaatkan oleh penyerang untuk merusak, mencuri informasi atau mengambil alih kendali situs web tersebut. Kerentanan *website* dapat diakibatkan oleh berbagai faktor, seperti kurangnya pengaturan keamanan, ketidakamanan kode, penggunaan plugin atau aplikasi yang tidak terbarui, dan lain-lain. Beberapa jenis kerentanan *website* yang umum di antaranya:

1. *SQL Injection*: adalah teknik untuk memanipulasi database *website* dengan memasukkan query SQL yang berbahaya.
2. Cross-site scripting (XSS): adalah serangan yang memungkinkan penyerang menyisipkan kode berbahaya ke dalam halaman web, yang dapat menyebabkan kerentanan pada browser pengunjung.
3. Cross-site request forgery (CSRF): adalah serangan yang mengirimkan permintaan palsu dari situs web yang tepercaya ke situs web yang rentan,

yang memungkinkan penyerang untuk mengirimkan permintaan berbahaya.

4. DDoS (*Distributed Denial of Service*): adalah serangan yang membanjiri server dengan lalu lintas web palsu untuk membuat situs web menjadi tidak dapat diakses oleh pengguna yang sah.

Penting untuk mengambil langkah-langkah keamanan yang tepat untuk melindungi situs web dari kerentanan. Beberapa langkah yang dapat dilakukan antara lain menggunakan perangkat lunak keamanan, memperbaharui plugin atau aplikasi yang digunakan secara teratur, dan mengikuti praktik keamanan yang baik seperti penggunaan password yang kuat dan kompleks serta melakukan backup secara teratur.

2.1.2 Serangan Jaringan

Serangan jaringan merupakan sebuah insiden dimana sebuah jaringan pada komputer atau *website* akan mengalami sebuah anomali. Ada banyak serangan jenis serangan jaringan namun penelitian ini akan menguji 4 jenis serangan yang dapat terjadi pada Aplikasi Web.

2.1.2.1 *SQL Injection*

SQL Injection merupakan serangan yang dilakukan dengan cara mengirim data yang tidak valid kedalam aplikasi web dengan tujuan agar aplikasi web melakukan sesuatu yang tidak seperti biasanya saat dirancang diawal. *Injection* sering terjadi dalam *query* SQL atau biasa disebut dengan serangan *SQL Injection* [4]. Ada beberapa jenis serangan injection ini antara lain adalah *Union SQL Injection, Blind SQL Injection, Error – based SQL Injection, Stacked Query SQL Injection, In-Band SQL Injection,* dan masih banyak lagi. Tentunya serangan ini akan memanfaat kan celah kerentanan dari suatu kode didalam database sehingga nantinya penyerang dapat memasuki dengan mudah database tersebut. Berikut adalah beberapa scenario serangan *SQL Injection* :

1. Mengambil data pengguna: Seorang penyerang dapat memasukkan kode SQL ke dalam input data yang dimasukkan oleh pengguna pada aplikasi

web dan mengambil data pengguna, seperti nama pengguna, alamat email, dan kata sandi.

2. Memodifikasi data: Seorang penyerang dapat memasukkan kode SQL ke dalam input data pada aplikasi web untuk memodifikasi data yang tersimpan di database, seperti mengubah informasi pengguna atau menghapus data.
3. Membuat akun administrator: Seorang penyerang dapat memasukkan kode SQL ke dalam input data pada aplikasi web untuk menciptakan akun administrator yang baru dan mengambil alih kontrol atas sistem.
4. Menghapus database: Seorang penyerang dapat memasukkan kode SQL ke dalam input data pada aplikasi web untuk menghapus seluruh database dan semua data yang disimpan di dalamnya.
5. Mencuri data sensitif: Seorang penyerang dapat memasukkan kode SQL ke dalam input data pada aplikasi web untuk mencuri data sensitif, seperti nomor kartu kredit, nomor identitas, atau data medis.
6. Mengungkapkan informasi sistem: Seorang penyerang dapat memasukkan kode SQL ke dalam input data pada aplikasi web untuk mengungkapkan informasi tentang sistem, seperti versi sistem operasi, versi database, dan informasi lainnya yang dapat membantu penyerang untuk merancang serangan yang lebih lanjut.

Penting untuk selalu memastikan bahwa aplikasi web terlindungi dari serangan *SQL Injection* dengan memvalidasi input data yang masuk dan menggunakan *parameterized query*.

2.1.2.2 DDoS Attack

Distributed Denial of Service (DDoS) merupakan serangan yang melakukan percobaan untuk membuat suatu *website* tidak dapat diakses atau membuat *website* memiliki *load* beban yang berat sehingga lambat untuk diakses oleh pengguna dengan mengirim banyak permintaan yang berlebihan dalam waktu yang sangat berdekatan. Untuk serangan ini memang terlihat remeh, namun dampak negative serangan ini cukup besar karena dapat membuat kerugian

finansial bagi suatu perusahaan atau organisasi dan membuat citra negative kepada pengguna atau pelanggan dari organisasi tersebut. Ada beberapa jenis serangan DDoS ini antara lain yaitu TCP Flood, UDP Flood, ICMP Flood, dan HTTP Flood. Berikut beberapa skenario serangan ini :

1. Penyerang menggunakan botnet (sebuah jaringan komputer yang dikendalikan oleh malware) untuk mengirimkan ribuan bahkan jutaan permintaan ke sumber daya yang diserang dalam waktu yang singkat. Permintaan ini kemudian akan membanjiri server, membuatnya kehabisan sumber daya, dan membuatnya tidak dapat menangani permintaan yang sah.
2. Serangan DDoS bisa dilakukan menggunakan berbagai jenis teknik seperti UDP flood, SYN flood, HTTP flood, dan amplification attack. Misalnya, pada UDP flood, penyerang akan mengirimkan banyak permintaan ke server dengan port UDP yang berbeda-beda, sementara pada SYN flood, penyerang akan mengirimkan permintaan SYN palsu untuk mencoba mengeksploitasi kerentanan di server dan membuatnya tak berfungsi.
3. Penyerang mungkin juga memanfaatkan teknik spoofing untuk menyembunyikan asal lalu lintas mereka dan membuat sulit bagi sistem pertahanan untuk mengidentifikasi sumber serangan.
4. DDoS seringkali digunakan sebagai alat untuk mencoba memeras uang dari sumber daya yang diserang dengan cara meminta pembayaran tebusan untuk menghentikan serangan.
5. Untuk mengatasi serangan DDoS, ada beberapa taktik yang bisa dilakukan, misalnya memblokir alamat IP yang mencurigakan, menggunakan solusi anti-DDoS, atau meningkatkan keamanan infrastruktur sistem dengan *firewall* dan *software* pengaman lainnya.

2.1.2.3 *Cross-Site Scripting (XSS)*

Cross-Site Scripting atau biasa disebut XSS merupakan salah satu serangan yang sangat berbahaya namun sebagian besar korban tidak menyadari sedang

diserang oleh serangan jenis ini [5]. XSS adalah serangan yang dilakukan dengan cara memasukan *malicious script code* kedalam suatu *aktivitas* dan memaksa aktivitas itu untuk menjalankan *script* tersebut. Dampak dari serangan ini antara lain seperti pencurian *cookie* dari *document.cookie* dalam *aktivitas*, melakukan redirect pengguna aktivitas kedalam *evil site*, terjadinya serangan DoS pada aktivitas, hingga *phising* yang sangat berbahaya. Berikut beberapa skenario dari serangan xss ini :

1. Penyerang mengirimkan email phishing ke pengguna dengan tautan ke situs web yang terinfeksi. Tautan ini mungkin terlihat seperti tautan yang sah, seperti tautan ke layanan bank atau situs jejaring sosial.
2. Jika pengguna mengklik tautan tersebut, maka situs web yang terinfeksi akan dimuat. Situs web tersebut dapat memuat skrip jahat yang mengambil informasi sensitif pengguna, seperti nama pengguna dan kata sandi, atau memuat iklan yang tidak diinginkan atau halaman phishing palsu.
3. Skrip jahat yang disisipkan oleh penyerang dapat memungkinkan mereka untuk mengambil alih sesi pengguna, yang memungkinkan mereka untuk mengakses informasi sensitif atau melakukan tindakan di situs web atas nama pengguna.
4. Penyerang juga dapat menggunakan skrip jahat untuk mengambil cookie atau token otentikasi pengguna, yang memungkinkan mereka untuk masuk ke situs web tanpa perlu memasukkan informasi login.

Untuk mencegah serangan skrip lintas situs, aplikasi web harus memvalidasi dan membersihkan input pengguna sebelum menampilkannya kembali ke pengguna. Selain itu, aplikasi web harus menyertakan input pengguna dalam tanda kutip dan menyandikan karakter khusus yang digunakan dalam HTML, seperti < dan >, untuk mencegah penyerang menyisipkan skrip berbahaya. Terakhir, pengguna harus diperingatkan untuk tidak mengklik tautan yang mencurigakan atau mengunduh file yang tidak dikenal.

2.1.3 Intruction Prevention/Detection System (IPS/IDS)

Intrusion Prevention/detection system merupakan alat teknologi jaringan yang dapat mencegah dan merekam suatu yang mencurigakan dalam suatu lalu lintas jaringan, nantinya jika IPS/IDS ini menemukan atau mendeteksi hal yang mencurigakan, IPS/IDS akan memberi peringatan administrator jaringan serta dapat mencegah serangan tesebut terulang [7]. Ada beberapa jenis IPS/IDS yang umum digunakan diantaranya adalah sebagai berikut :

1. *Host-based* IPS/IDS: teknologi IPS/IDS ini dipasang pada perangkat host individu, seperti server atau workstation, dan bekerja untuk melindungi perangkat dari serangan berbasis jaringan.
2. *Network-based* IPS/IDS: teknologi IPS/IDS ini dipasang pada jaringan, seperti router atau firewall, dan bekerja untuk melindungi jaringan dari serangan berbasis jaringan.
3. *Signature-based* IPS/IDS: teknologi IPS/IDS ini menggunakan database signature untuk mengidentifikasi serangan yang dikenal dan memblokirnya.
4. *Anomaly-based* IPS/IDS: teknologi IPS/IDS ini menggunakan machine learning untuk memantau perilaku jaringan dan mendeteksi aktivitas yang tidak biasa atau mencurigakan.
5. *Hybrid* IPS/IDS: teknologi IPS/IDS ini menggabungkan beberapa jenis deteksi untuk memberikan tingkat perlindungan yang lebih tinggi dan lebih efektif.
6. *Protocol-based* IPS/IDS: teknologi IPS/IDS ini dipasang pada level protokol dan berfungsi untuk mencegah serangan yang menargetkan protokol jaringan yang spesifik.
7. *Application-based* IPS/IDS: teknologi IPS/IDS ini berfokus pada deteksi dan pencegahan serangan yang berhubungan dengan aplikasi atau layanan tertentu yang berjalan di jaringan.

Setiap jenis IPS/IDS memiliki kelebihan dan kekurangan tersendiri, dan organisasi perlu mempertimbangkan kebutuhan keamanan mereka sebelum memilih teknologi yang tepat untuk diimplementasikan. Disini nantinya penulis

akan menggunakan jenis yang pertama yaitu host base karena hampir setiap penyerang sebuah aplikasi web akan memikirkan segala cara untuk berhasil melakukan sebuah serangan maka IPS/IDS host base masih sangat cocok untuk digunakan.

Ada beragam aplikasi IPS/IDS yang digunakan dalam jaringan saat ini yang umum digunakan dan berikut merupakan aplikasi – aplikasinya :

1. Snort: Snort adalah salah satu aplikasi IDS open-*source* yang paling populer dan banyak digunakan. Snort mendeteksi serangan dengan cara memonitor lalu lintas jaringan dan mencocokkan pola dengan database serangan yang telah diketahui.
2. Suricata: Suricata adalah aplikasi IDS open-*source* lainnya yang berfungsi dengan cara yang mirip dengan Snort. Suricata dapat mendeteksi serangan dengan mengawasi lalu lintas jaringan dan menganalisis paket jaringan.
3. OSSEC: OSSEC adalah aplikasi IDS open-*source* yang berfokus pada deteksi ancaman pada sistem operasi. OSSEC mengumpulkan informasi dari file log dan sistem, dan memeriksa informasi tersebut untuk mencari tanda-tanda serangan.
4. Cisco Firepower: Cisco Firepower adalah produk komersial yang menyediakan kombinasi antara IDS dan IPS. Cisco Firepower memiliki kemampuan untuk mendeteksi serangan dan mencegah serangan dengan memblokir lalu lintas yang mencurigakan.
5. McAfee Network Security Platform: McAfee Network Security Platform adalah produk komersial yang memiliki kemampuan IDS/IPS. McAfee Network Security Platform dapat mendeteksi serangan dan mencegah serangan dengan memblokir lalu lintas yang mencurigakan.
6. Check Point IPS: Check Point IPS adalah produk IPS komersial yang berfokus pada keamanan jaringan. Check Point IPS dapat mendeteksi serangan dan mencegah serangan dengan memblokir lalu lintas yang mencurigakan.

7. TippingPoint IPS: TippingPoint IPS adalah produk IPS komersial yang menyediakan perlindungan keamanan untuk jaringan dan aplikasi. TippingPoint IPS dapat mendeteksi serangan dan mencegah serangan dengan memblokir lalu lintas yang mencurigakan.
8. Palo Alto Networks: Palo Alto Networks adalah produk keamanan jaringan komersial yang menyediakan fitur IDS dan IPS. Palo Alto Networks dapat mendeteksi serangan dan mencegah serangan dengan memblokir lalu lintas yang mencurigakan.

Sebetulnya masih banyak lagi aplikasi lain yang dapat digunakan untuk mendeteksi dan mencegah serangan jaringan. Untuk kali ini, penulis akan menggunakan aplikasi snort untuk dilakukan implementasi pada penelitian ini.

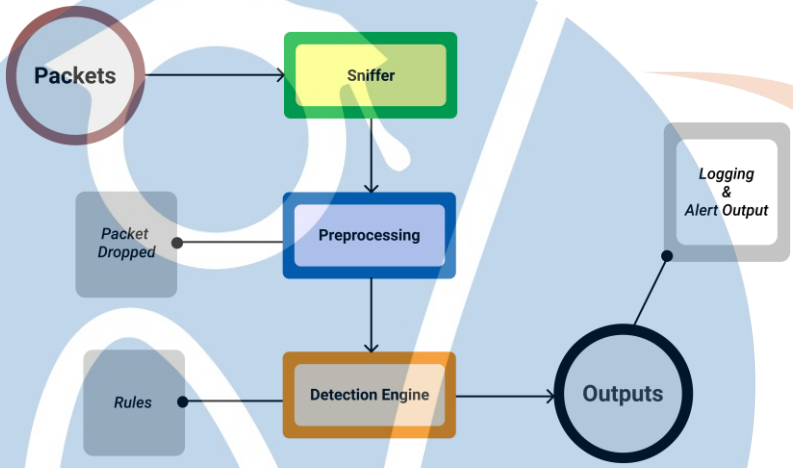
2.1.3.1 Snort

Snort merupakan IDS yang bersifat *open source*. Alat ini memiliki komponen – komponen yang dapat bekerja sama untuk mendeteksi sesuatu yang mencurigakan dalam jaringan dan akan menghasilkan *output* dalam format yang diperlukan oleh sistem pendeteksi. Alat ini juga dirancang untuk dapat melakukan *cross platform* [8]. Kekurangan alat ini yaitu berbasis *command line* karena dapat memperberat proses analisa terhadap serangan ke suatu jaringan.

Snort bekerja secara *real-time* terhadap lalu lintas jaringan dan paket – paket yang melalui jaringan tersebut. Pada sistem ini snort melakukan analisa terhadap *protocol* dan konten dengan pola – pola serangan umum yang sudah ada dan snort memiliki 3 mode umum untuk mendeteksi pola – pola serangan umum, diantaranya yaitu ;

- Packet Sniffer, pada mode ini snort akan melakukan pembacaan paket dari network kemudian ditampilkan dalam bentuk continuos stream pada console screen atau layar terminal
- Packet Logger, pada mode ini snort akan mencatat semua paket yang lewat dalam jaringan dan nantinya paket tersebut akan menjadi bahan untuk analisa snort

- Intrusion Detection Mode, pada mode ini snort akan melakukan proses pendeteksian terhadap paket – paket yang telah tercatat yang dilakukan melalui jaringan komputer. Snort akan melakukan pendeteksian sesuai dengan rules yang telah dibuat.



Gambar 2. 1 Snort Workflow

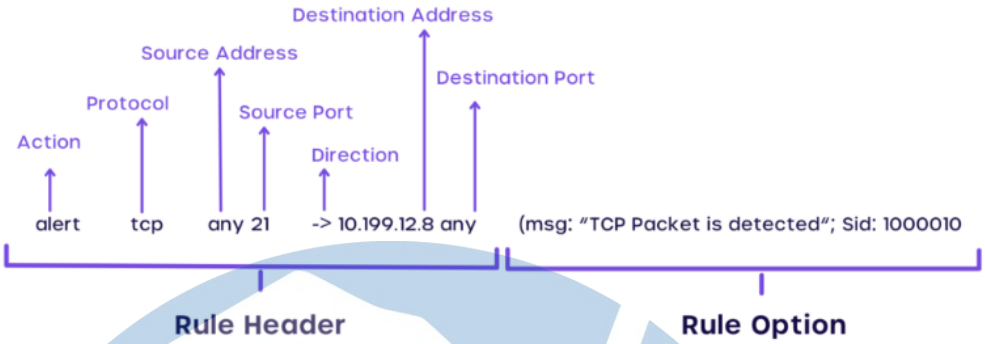
Perhatikan gambar diatas, gambar tersebut merupakan gambar dari arsitektur snort. Karena merupakan sebuah IDS maka nantinya snort akan menghasilkan sebuah output yang dibutuhkan oleh admin jaringan. berikut penjelasan dari gambar arsitektur snort ;

- Packets, pada proses ini sistem didalam snort akan data yang melalui Ethernet card dan selanjutnya akan diterima oleh sniffer
- Sniffer, pada proses ini sniffer akan menerima data yang sudah dicapture oleh tahap sebelumnya melalui layer 2 atau layer data link untuk mendapatkan informasi *protocol* yang dapat diproses lebih lanjut.

- Preprocessing, proses ini merupakan proses analisa terhadap data serta melakukan manipulasi sebelum dikirim ke detection engine, manipulasi data ini dapat berupa penandaan, pengelompokan, hingga dihentikan.
- Detection Engine, pada proses data – data yang sudah disalurkan oleh preprocessing akan dibandingkan dengan rules yang telah dibuat oleh seorang administrator, rules ini berisi signature atau tanda – tanda seperti serangan jaringan.
- Outputs, merupakan proses akhir dari snort dalam melakukan pendeteksian terhadap paket paket data yang lewat dalam jaringan, proses ini akan menghasilkan keluaran dari detection engine atau bisa dibilang log dan alert

Untuk mendeteksi suatu serangan snort akan membaca sebuah pola serangan jaringan dengan disesuaikan dengan konfigurasi pada rule yang sudah dibuat. Rule snort merupakan sebutan dari aturan yang digunakan untuk melakukan identifikasi terhadap serangan atau aktivitas merugikan pada sebuah jaringan. Rule snort terdiri dari beberapa bagian yang utama antara lain yaitu :

- *Header Rule*, merupakan bagian rule yang digunakan untuk menentukan jenis protokol yang akan diawasi.
- *Options Rule*, merupakan bagian rule yang digunakan untuk menentukan kondisi – kondisi tertentu yang harus terpenuhi sebelum aturan dapat diterapkan.
- *Content Rule*, merupakan bagian rule yang digunakan untuk mengidentifikasi pola data tertentu yang mecurigakan dan harus dicocokan dengan data atau aktivitas yang sedang dipantau.

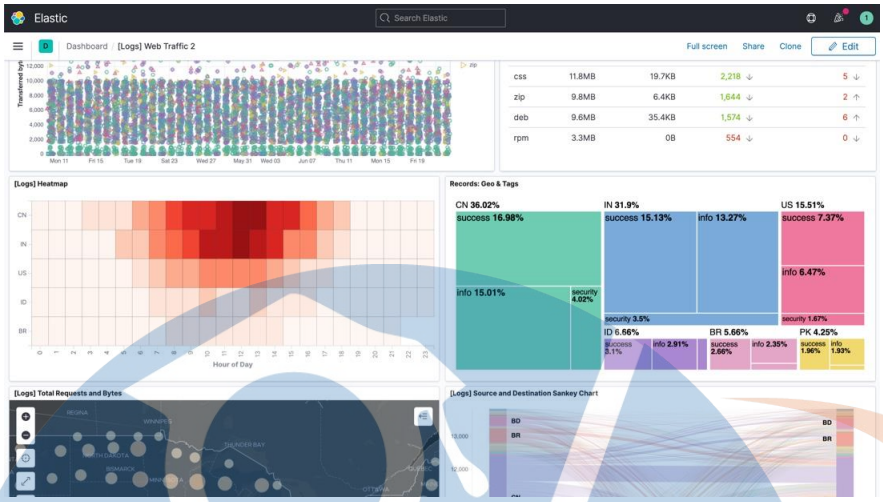


Gambar 2. 2. Rule Snort

Secara umum, rule Snort terdiri dari beberapa komponen yaitu *action*, *protocol*, *source address*, *source* port, direction, *destination address*, *destination* port, dan *content*. *Action* menentukan tindakan apa yang harus dilakukan jika aturan tersebut terpenuhi. *Protocol* menentukan protokol yang harus dipantau, sedangkan *source address* dan *destination address* menentukan alamat IP sumber dan tujuan. *Source* port dan *destination* port menentukan port yang digunakan oleh sumber dan tujuan. Direction menentukan arah lalu lintas yang harus dipantau. Content berisi pola data tertentu yang harus dicocokkan dengan data yang sedang dipantau.

2.1.4 Sistem Dashboard

Sistem dashboard merupakan aplikasi berbentuk aktivitas atau sistem informasi yang menyediakan infomasi dari kinerja, hasil, maupun evaluasi dari sebuah perusahaan atau organisasi dengan maksud untuk memudahkan aktivitas monitoring dari kinerja, sistem ini sudah banyak diterapkan dalam berbagai perusahaan atau organisasi [6]. Pada penelitian ini sistem dashboard akan menggunakan kibana dan akan memvisualisasikan data serangan yang sudah diintegrasi oleh elasticseach dan logstash.



Gambar 2. 3. Sistem Dashboard Menggunakan Kibana

2.1.5 ELK Stack

ELK Stack merupakan perkumpulan dari beberapa aplikasi *open source* yang digabungan dengan tujuan untuk mempermudah pengolahan data yang memiliki volume sangat besar [7]. Isi dari ELK Stack itu sendiri antara lain, Elasticsearch, Logstash, dan Kibana. Dalam ELK Stack, Logstash akan melakukan penarikan data yang akan diolah, data yang sudah ditarik lalu diurai serta diurutkan. Setelah itu, Elasticsearch akan melakukan indeks data. Terakhir, data yang telah terindeks akan divisualisasikan oleh Kibana.

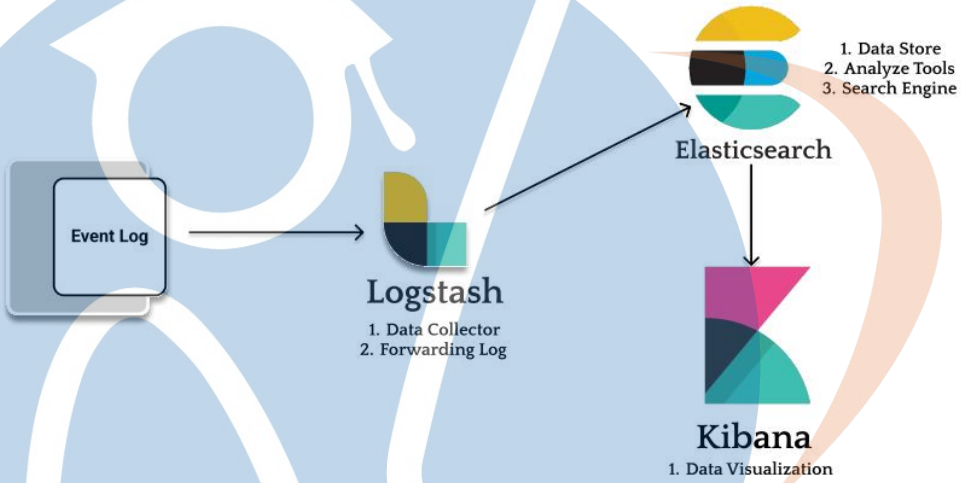
2.1.5.1 Elasticsearch

Elasticsearch adalah sebuah aplikasi *open source* untuk mencari dan menganalisa berbagai jenis data yang berbasis pada Apache Lucene [11]. Elasticsearch akan melakukan pemrosesan data yang awal nya mentah kemudian diuraikan lalu dinormalisasikan dan kemudian data tersebut dikuatkan oleh data – data tambahan sebelum dilakukan proses indeks pada data tersebut. Aplikasi ini bersifat *scalable* sehingga dapat mudah untuk dikembangkan tergantung dengan kebutuhan yang ada. Elasticsearch menyimpan data dengan bebasis dokumen dan sangat berbeda dengan berbasis table atau yang biasa kita kenal RDBMS, pada aplikasi ini data disimpan dengan berorientasikan dokumen lalu disimpan sebagai JSON yang

terstruktur dan dilakukan pada setiap bidang indeks secara *default*. Sehingga Elasticsearch mampu melakukan proses pencarian data kecepatan yang sangat luar biasa. Berikut fitur – fitur yang ada pada elasticsearch :

1. Skalabilitas: Elasticsearch dirancang untuk bisa melakukan scaling secara horizontal, yang memungkinkan pengguna untuk menambahkan node secara mudah saat kebutuhan meningkat.
2. Pencarian: Elasticsearch menyediakan fitur pencarian yang sangat cepat dan akurat untuk memproses data yang sangat besar. Fitur ini dilengkapi dengan fitur full-text search, pencarian fuzzy, pencarian gabungan, dan lainnya.
3. Analisis: Elasticsearch menyediakan fitur analisis yang lengkap, termasuk pemrosesan teks dan analisis struktural data, sehingga pengguna dapat memproses dan menganalisis data dengan lebih efektif.
4. Indexing: Elasticsearch menggunakan teknologi Lucene untuk membangun index yang sangat efisien dan cepat. Pengguna dapat membuat index yang terdiri dari satu atau banyak field dan melakukan indexing data dalam jumlah besar.
5. Ketersediaan dan Ketahanan: Elasticsearch memiliki fitur ketersediaan dan ketahanan yang sangat baik dengan memanfaatkan teknologi replikasi dan alokasi otomatis.
6. Agregasi: Elasticsearch dapat melakukan agregasi data dalam jumlah besar dengan menggunakan fitur aggregasi seperti sum, avg, max, dan min.
7. RESTful API: Elasticsearch menyediakan RESTful API yang memungkinkan pengguna untuk berinteraksi dengan Elasticsearch melalui HTTP dengan mudah.
8. Integrasi: Elasticsearch dapat diintegrasikan dengan berbagai macam teknologi dan platform seperti logstash, beats, Kibana, dan banyak lagi.

9. Kemampuan Visualisasi: Elasticsearch memungkinkan pengguna untuk membuat grafik dan visualisasi yang indah dan informatif dari data yang diindeks.
10. Keamanan: Elasticsearch memiliki fitur keamanan yang lengkap, termasuk otentikasi, otorisasi, dan enkripsi data.



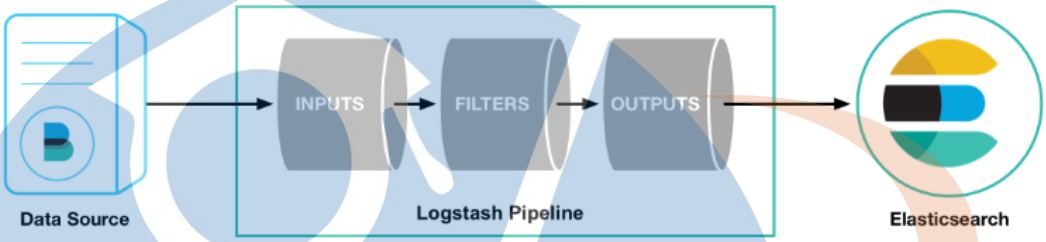
Gambar 2. 4 ELK Stack Workflow

2.1.5.2 Logstash

Logstash adalah aplikasi yang penting dalam ELK Stack, itu dikarenakan Logstash yang akan berperan melakukan proses penarikan dan pengumpulan data yang akan digunakan dalam Elasticsearch [12]. Logstash juga berkemampuan melakukan *pipelining* secara *realtime* pada data yang akan diteruskan kedalam Elasticsearch. Untuk mendapatkan masukan data yang tepat Logstash memerlukan sebuah konfigurasi. Konfigurasi dalam aplikasi ini terdapat 3 tahapan yaitu *input*, *filter*, *output*, dan tiap tahapan ini memiliki *plugin* yang berfungsi sebagai pembantu dari Logstash itu sendiri. Berikut fitur – fitur utama pada logstash :

1. Input: Logstash menyediakan berbagai macam plugin input, seperti file input, TCP/UDP input, stdin input, dan masih banyak lagi. Plugin-plugin ini memungkinkan Logstash untuk menerima data log dari berbagai sumber.
2. Filter: Logstash juga menyediakan plugin filter yang dapat digunakan untuk memproses dan mengubah data log. Beberapa plugin filter yang tersedia diantaranya Grok, Date, Mutate, dan masih banyak lagi. Plugin-filter ini memungkinkan pengguna untuk memperbaiki format data, memperkaya data, mengekstrak informasi penting dari data log, dan masih banyak lagi.
3. Output: Setelah data log diproses dan diubah oleh plugin-filter, Logstash dapat mengirimkannya ke berbagai tujuan output, seperti Elasticsearch, Kafka, Redis, atau bahkan ke sistem penyimpanan file seperti S3. Plugin-plugin output yang tersedia di Logstash memungkinkan pengguna untuk mengirim data ke berbagai sistem atau layanan.
4. Scalability: Logstash dapat dijalankan dalam mode *distributed* (berdistribusi) dan memiliki fitur auto-discovery, yang memungkinkan kinerja dan skala Logstash diatur sesuai dengan kebutuhan.
5. Plugin-based architecture: Logstash dirancang dengan arsitektur berbasis plugin, yang memungkinkan pengguna untuk menambahkan atau menghapus plugin-plugin sesuai dengan kebutuhan mereka.
6. Ketersediaan yang Tinggi: Logstash memungkinkan replikasi dan sinkronisasi antar node untuk memastikan ketersediaan yang tinggi dari data log.
7. Monitoring: Logstash menyediakan antarmuka monitoring, yang memungkinkan pengguna untuk memonitor kinerja dan kesehatan Logstash dan sistem yang terintegrasi dengannya.
8. Konfigurasi yang fleksibel: Logstash menggunakan format konfigurasi yang mudah dipahami dan diubah sesuai dengan kebutuhan pengguna.

9. Community-driven: Logstash adalah perangkat lunak open-*source* yang didukung oleh komunitas pengembang dan pengguna yang aktif dan berkembang. Ini memungkinkan pengguna untuk memperoleh dukungan dan kontribusi yang kaya dan terus berkembang dari komunitas.



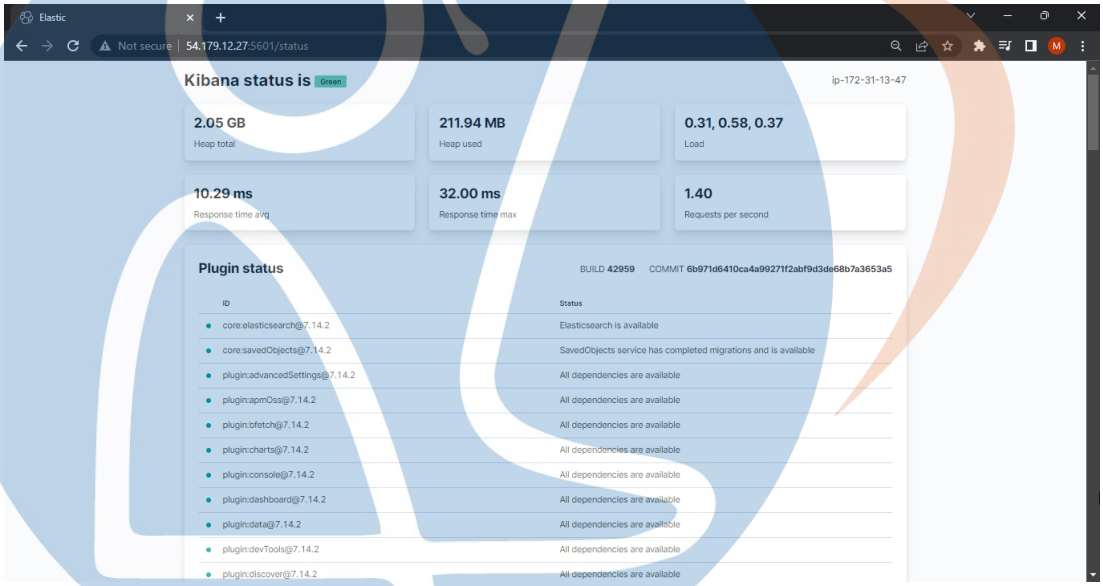
Gambar 2. 5 Pipelining Logstash

2.1.5.3 Kibana

Kibana merupakan aplikasi didalam ELK Stack yang berfungsi untuk memvisualisasikan data yang telah dikumpulkan dan diolah pada Logstash dan Elasticsearc [13]. Data yang divisualisasi dapat berbentuk gambar, tabel, grafik, higga *metric* dalam halaman *dashboard* yang sudah menjadi salah satu fitur dalam kibana. Berikut beberapa fitur – fitur kibana :

1. Visualisasi Data: Kibana memungkinkan pengguna untuk membuat visualisasi data yang menarik, termasuk grafik, tabel, peta, dan diagram yang dapat ditampilkan dalam bentuk dashboard.
2. Penjelajahan Data: Kibana memungkinkan pengguna untuk melakukan pencarian, penjelajahan, dan pemfilteran data secara interaktif, menggunakan berbagai jenis data seperti log, metrik, dan data lainnya.
3. Alerting: Kibana memungkinkan pengguna untuk membuat aturan pengingat dan alarm yang dapat membantu mengawasi kinerja dan kondisi sistem.
4. Integrasi: Kibana dapat diintegrasikan dengan berbagai jenis aplikasi dan layanan, termasuk Amazon Web Services (AWS), Google Cloud Platform (GCP), dan Microsoft Azure.

5. Machine Learning: Kibana juga memiliki fitur machine learning yang memungkinkan pengguna untuk membuat model prediksi dan melihat tren dalam data mereka.
6. Plugin: Kibana memiliki sistem plugin yang memungkinkan pengguna untuk menambahkan fitur tambahan seperti pengelolaan user, autentikasi, dan lainnya.
7. Kibana API: Kibana menyediakan API yang dapat digunakan untuk memanipulasi data dan konfigurasi Kibana secara programatik.



Gambar 2. 6 Kibana Status Dashboard

2. 2 Penelitian Terkait

Pada penelitian ini, penulis akan melakukan perbandingan dari beberapa penelitian yang terkait berdasarkan masalah yang penulis ambil. Dari beberapa penelitian yang dibandingkan terdapat beberapa dasar yang sama terkait pandangan terhadap Sistem monitoring serangan jaringan, dan juga visualisasi data dan analisa dengan menggunakan ELK Stack. Berikut ini merupakan beberapa dari penelitian terkait yang digunakan oleh peneliti ;

2. 3 Table Penelitian Terkait

Berikut adalah table yang membahas penelitian terkait dengan jumlah empat penelitian yang penulis ambil untuk dijadikan sebagai referensi rujukan :

Tabel 2. 1 Penelitian Terkait

No	Judul Penelitian	Penelitian	Kesimpulan
1	Implementasi Elasticsearch Logstash Kibana Stack ada Sistem Portal Pengembangan dan Pembinaan Sumber Daya Manusia	Elang Putra Sartika, Andhik Budi Cahyono. 2020 Fakultas Teknologi Industri Universitas Islam Indonesia, Yogyakarta, Indonesia.	Pada Penelitian ini, ELK Stack digunakan untuk meningkatakan kinerja dari sistem portal PPSDM agar dapat menggambil keputusan dengan tepat. Pada penelitian ini juga menjelaskan beberapa kemampuan dari ELK Stack dan cara untuk memanfaatkan kemampuan tersebut yang antara lain yaitu memanfaatkan API ELK Stack untuk mencari sebuah data dan juga memanfaatkan Kibana sebagai sistem dashboard yang diperlukan untuk monitoring.
2	Sistem Monitoring Serangan Jaringan Komputer Berbasis Web Service Menggunakan Honeypot Sebagai Intrusion Prevention System	Indah Sari, Muh Yamin, LM. Fid Aksara. 2019 Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari	Pada Penelitian ini, Sistem Monitoring menagandalkan Honeypot sebagai IPS nya, yang dapat mengenali *port* TCP, UDP, ICMP, serta dapat mendeteksi anomali terhadap sistem. IPS sendiri yaitu sebuah sistem pengembangan dari IDS

No	Judul Penelitian	Penelitian	Kesimpulan
3	Analisi Monitoring Sistem Keamanan Jaringan Komputer Menggunakan *Software* NMAP (Studi Kasus di SMK Negeri 1 Kota Serang)	Dwi Bayu Rendro, Ngatono, Wahyu Nugroho Aji. 2020 Rekayasa Sistem Komputer, Fakultas Teknologi Informasi, Universitas Serang Raya	Pada Penelitian ini lebih mengarah ke sebuah proses pentesting yang bertujuan melakukan pendeteksian sebuah kerentanan sebuah jaringan, penelitian ini menggunakan *tools* NMAP yang digunakan untuk pengujian mulai dari *scanning* jaringan yang berupa IP *address* dan aktivitas.
4	Perancangan Sistem Monitoring *Multiple Network* Menggunakan *Platform Elastic Stack* (Studi Kasus: PT. JEDI GLOBAL TEKNOLOGI)	Vian Handika. 2020 Program Studi Informatika, Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta	Pada penelitian ini, Sistem Monitoring tehadap jaringan dirancang menggunakan platform Elastic Stack dan membangun aplikasi android untuk menerima notifikasi ketika ada permasahalan dalam sistem monitoring nya.
5	Perancangan dan Implementasi Dashboard Monitoring dan Analisis Serangan Aplikasi Web Menggunakan ELK Stack	Muhammad Ilham. 2023 STT Terpadu Nurul Fikri, 2021.	Pada penelitian ini yaitu melakukan rancangan dashboard monitoring serangan terhadap aplikasi web dan melakukan analisa serangan menggunakan dashboard monitoring yang menggunakan ELK Stack dengan melakukan shipping log dari alat pendeteksian serangan (IPS/IDS) kedalam ELK Stack

Pada penelitian pertama, berfokus kepada pemanfaatan dari kinerja ELK Stack yang memanfaatkan teknologi dari API ELK Stack dan Kibana untuk mengolah data dan menggunakannya untuk pengambilan keputusan dari sebuah porta PPSDM agar menjadi lebih tepat. Penelitian kedua, berfokus pada sebuah sistem monitoring yang dijadikan honey pot sebagai alat pendeteksiannya dan sistem pendeteksian tersebut melakukan scanning terhadap port TCP, UDP, dan ICMP. Penelitian ketiga, berfokus kepada pendeteksian serangan atau kerentanan sebuah jaringan menggunakan tools NMAP dengan melakukan pengujian dengan melakukan scanning terhadap IP *address* dan aktivitas. Penelitian keempat, berfokus kepada pembangunan sebuah sistem montiring menggunakan ELK Stack yang memantau aktivitas jaringan dari sebuah aktivitas menggunakan kibana dan melakukan perubahan dari alerting menjadi notifikasi pada aplikasi android. Pada penelitian ini, berfokus pada perancangan implementasi dashboard monitoring dan analisa serangan terhadap aplikasi web dengan menggunakan alat pendeteksian serangan jaringan atau IDS yaitu snort lalu menggunakan ELK Stack sebagai alat pengolah data dari log serangan tersebut lalu dijadikan sebagai dashboard agar dapat dianalisa.

2.3.1 Posisi penelitian

Tabel berikut bertujuan untuk menentukan posisi pada penelitian ini dari penelitian terkait yang sebelumnya telah dijelaskan:

Tabel 2. 2 Posisi Penelitian

No	Penelitian	Pendeteksian Serangan	Visualisasi Log	ELK	Analisa Serangan	Pengujian Fungsional
1	Implementasi Elasticsearch Logstash Kibana Stack ada Sistem Portal Pengembangan dan Pembinaan Sumber Daya Manusia Elang Putra Sartika, Andhik Budi Cahyono. 2020					
2	Sistem Monitoring Serangan Jaringan Komputer Berbasis Web Service Menggunakan Honeypot Sebagai Intrusion Prevention System Indah Sari, Muh Yamin, LM. Fid Aksara. 2019					
3	Analisi Monitoring Sistem Keamanan Jaringan Komputer Menggunakan *Software* NMAP (Studi Kasus di SMK Negeri 1 Kota Serang) Dwi Bayu Rendro, Ngatono, Wahyu Nugroho Aji. 2020					

No	Penelitian	Pendeteksian Serangan	Visualisasi Log	ELK	Analisa Serangan	Pengujian Fungsional
4	Perancangan Sistem Monitoring *Multiple Network* Menggunakan *Platform Elastic Stack* (Studi Kasus: PT. JEDI GLOBAL TEKNOLOGI) Vian Handika. 2020					
5	Perancangan dan Implementasi Dashboard Monitoring dan Analisis Serangan Aplikasi Web Menggunakan ELK Stack Muhammad Ilham. 2023					