BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Pada penelitian ini penulis melakukan tinjauan pustaka pada beberapa penelitian sebelumnya untuk mendukung penelitian yang sedang dilakukan. Berikut adalah tinjauan pustaka yang digunakan penulis yang dapat dilihat pada Tabel 2.1.

Tabel 2.1 Daftar Literatur

No	Penulis	Tahun	Judul Penelitian
1	Muhammad Rijal Kamal	2022	Implementasi *Security Information and Event Management* (SIEM) dengan *Splunk* untuk Analisis Tren Ancaman Siber pada Jaringan UII
2	Claudia Tarigan, Ventje Jeremias Lewi Engel, Dina Angela	2018	Sistem Pengawasan Kinerja Jaringan *Server Web Apache* dengan *Log Management System* ELK (*Elasticsearch, Logstash, Kibana*)
3	Muhammad Alfandi	2022	Analisa *Security Information and Event Management* (SIEM) Menggunakan *Elastic Stack* SIEM dan *Splunk*
4	Walidatush Sholihah	2020	*Log Event Management Server* Menggunakan *Elastic Search Logstash Kibana* (ELK *Stack*)
5	Muhamad Nur Arifin, Sugiartowo, Emi Susilowati	2018	Desain dan Implementasi *Log Event Management Server* Menggunakan *Elasticsearch Logstash Kibana* (ELK *Stack*)

Muhammad Rijal Kamal (2022) dari Informatika Fakultas Teknologi Industri Universitas Islam Indonesia dengan judul Implementasi *Security Information and Event Management* (SIEM) dengan *Splunk* untuk Analisis Tren Ancaman Siber pada Jaringan UII. Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang analisis pada *log firewall* dengan mengimplementasikan SIEM sebagai solusi untuk membantu menganalisis tren ancaman siber yang ada pada UII. *Log* tersebut diolah menggunakan *Splunk* yang mendukung pengolahan data secara besar yang dihasilkan *firewall* UII, Log diunggah dan dilakukan pencarian data sesuai *rules*, kemudian hasil pencarian akan divisualisasikan dan ditampilkan pada *dashboard*.

Berdasarkan data hasil dari pengujian pada penelitian ini didapat hasil dari threat yang sering masuk ke jaringan UII sebanyak 3.511.236 *events threat* dengan NONRFC *Compliant* SSL *Traffic on Port* 443 paling banyak dengan jumlah 1.124.058 *events*, hasil dari *rules vulnerability* sebanyak 2.162.260 *events vulnerability*, hasil dari *rules severity* menampilkan 1.223.811 *level critical* dengan *Coinminer Command and Control Trafic Detection* paling banyak ditemukan dengan jumlah 709.857. Hasil dari jumlah ancaman dan serangan berdasarkan tipe serangan diimplementasikan dengan SIEM *Splunk* berupa grafik yang dapat ditampilkan dan dibaca di *dashboard*.

Claudia Tarigan, Ventje Jeremias Lewi Engel, Dina Angela (2018) dari Teknologi Informasi Institut Teknologi Harapan Bangsa dengan judul Sistem Pengawasan Kinerja Jaringan *Server Web Apache* dengan *Log Management System* ELK (*Elasticsearch, Logstash, Kibana*). Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang cara mengintegrasikan

pengelolaan *Log Apache Web Server* ke dalam *log management system* ELK dan mengidentifikasi *performance indicator apache web server* dengan *log management* system ELK.

Berdasarkan data hasil dari pengujian pada penelitian ini adalah pengujian ART dengan rata-rata 79.55, pengujian PRT dengan rata-rata 91.186, pengujian CPU dengan rata-rata 999.953, dan pengujian Memori dengan rata-rata 4.048. Hasil dari Pengujian performa indikator menunjukkan perhitungan performa *web server*, yaitu waktu, *utilization*, dan *error*. Sehingga diperoleh hasil kinerja *uptime* terbesar 12,5 sedangkan ART mendapat hasil terkecil 2,72. Hal ini menunjukkan monitoring kinerja *Apache* menggunakan *log management system* perlu dilakukan untuk mengetahui pada waktu kapan saja *web server* banyak diakses oleh pengguna dan tidak *down.*

Muhammad Alfandi (2022) dari Informatika Fakultas Teknik Universitas Islam Riau Pekanbaru dengan judul Analisa *Security Information and Event Management* (SIEM) Menggunakan *Elastic Stack* SIEM dan *Splunk*. Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang pengujian serangan ke *server* berupa *Fingerprinting, SQL Injection, Denial of Service* (DoS) dan *Port Scanning*.

Berdasarkan data hasil dari pengujian pada penelitian ini *Elastic Stack* dan *Splunk* berhasil mendeteksi semua serangan yang terjadi selama 3 hari pengujian. Dengan hasil deteksi yang memiliki persamaan dan perbedaan untuk membantu dalam melakukan tindakan untuk mengatasi serangan yang terjadi. *Splunk* berhasil mengirimkan notifikasi semua serangan yang terjadi melalui *email* ke *administrator* sedangkan *Elastic Stack* gagal dalam mengirimkan notifikasi ke *administrator.*

Walidatush Sholihah (2020) dari Teknik Komputer Sekolah Vokasi IPB *University* dengan judul *Log Event Management Server* Menggunakan *Elastic Search Logstash Kibana* (ELK *Stack*). Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang pembuatan *log event* management *server* menggunakan ELK *Stack* yang dapat mempermudah dalam membaca dan menganalisis *log* pada *server*.

Berdasarkan data hasil dari pengujian pada penelitian ini menggunakan *CentOS7* sebagai *server client* dengan ssh yang sudah terpasang. Pengujian dilakukan dengan memasukkan *username* dan *password* yang salah secara berulang, hasil semua kegagalan dan keberhasilan dapat ditampilkan oleh *Kibana*. Pegujian penghapusan *log* pada *client* tidak menimbulkan pengaruh yang signifikan yang artinya tidak terjadi perubahan sedikitpun. Pengujian melakukan *bruteforce attack* ke *server* sebanyak 100 kali dengan hasil semua serangan dapat dilihat anomali pergerakan di *Kibana*. Hasil percobaan menunjukkan semua *log* dapat dikirimkan secara *realtime* ke *server* berhasil.

Muhamad Nur Arifin, Sugiartowo, Emi Susilowati (2018) dari Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jakarta dengan judul Desain dan Implementasi *Log Event Management Server* Menggunakan *Elasticsearch Logstash Kibana* (ELK *Stack*). Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang perancangan untuk membangun *Log Event Management Server* menggunakan ELK *Stack* untuk membaca dan menganalisis log *services* pada server *CentOS7* dan *Ubuntu* 14 dengan SSH *services* yang terpasang.

Berdasarkan data hasil dari pengujian pada penelitian ini yaitu pada pengujian pertama yaitu kesalahan *login password ssh* pada setiap *server client* dengan hasil semua kegagalan *login* dapat dilihat langsung masuk ke dalam *dashboard kibana*. Pengujian kedua yaitu kesalahan *login ssh* dengan *username* yang tidak terdapat pada *server client* sehingga akan terjadi kesalahan login *username* "asal-asal", hasil yang terlihat pada *kibana* adalah bertambahnya *username* di grafik *kibana*. Pengujian ketiga melihat tingkat akurasi waktu antara terjadinya kejadian kesalahan *login ssh* dan masuk *log* nya pada ELK *stack*, dengan hasil yang didapat adalah waktu sama dengan waktu kejadian kesalahan *login ssh* tersebut. Pengujian keempat dengan menghapus semua *log* yang terjadi pada *server* dan melihat pengaruh visualisasi yang terjadi di *server*, hasil yang terjadi adalah tidak ada perubahan sedikitpun pada grafiknya sehingga menandakan tidak berpengaruh penghapusan *log* yang sudah terjadi pada *server*. Hasil pengujian yang dibangun menunjukkan bahwa semua *log services* SSH yang terjadi pada *server client* dapat dikirimkan secara *realtime* ke *server* utama ELK *Stack* sekalipun isi *file log* pada *server* dihapus.

2.2 Keaslian Penelitian

Adapun beberapa hal yang menjadi pembeda antara penelitian yang dilakukan penulis dengan penelitian yang sudah pernah dilakukan sebelumnya sebagaimana terlampir di tabel tinjauan pustaka, antara lain ialah:

1) Penelitian ini menggunakan tiga macam serangan untuk menguji *Splunk* dan *Elastic Stack*, yaitu *Denial of Service* (DoS) *Attack*, *Port Scanning* dan *Bruteforce Attack*.

2) Penelitian ini berfokus terhadap kecepatan *ingest log*, deteksi *alert* serangan, waktu notifikasi *alert* dan penggunaan *resource* komputer.

Berikut adalah hasil perbandingan penelitian dari literatur sebelumnya.

No	Judul	Oleh	Tahun	General Ide	Hasil	Kelebihan	Kelemahan	Perbandingan
1	Sistem Pengawasan Kinerja Jaringan *Server Web Apache* dengan *Log Management System* ELK (*Elasticsearch, Logstash, Kibana*)	Claudia Tarigan, Ventje Jeremias Lewi Engel, Dina Angela	2018	Mengintegrasikan pengelolaan *Log Apache Web Server* ke dalam *log management system* ELK dan mengidentifikasi *performance indicator.*	Pengujian ART dengan rata-rata 79.55, pengujian PRT dengan rata-rata 91.186, pengujian CPU dengan rata-rata 999.953, dan pengujian Memori dengan rata-rata 4.048	Menggunakan *log management system* ELK terdiri dari *Elasticsearch, logstash, kibana* yang berintegrasi untuk di visualisasikan. Hasil berupa tiga indicator performa yaitu waktu, *utilization* dan *error*.	Kurangnya monitoring pada firewall, database pada *log management system* ELK.	Menggunakan SIEM *Splunk* sebagai perbandingan monitoring log pada server SIEM. Parameter pengujian berupa deteksi serangan, dan penggunaan *resource* komputer.

No	Judul	Oleh	Tahun	General Ide	Hasil	Kelebihan	Kelemahan	Perbandingan
2	Desain dan Implementasi *Log Event Management Server* Menggunakan *Elasticsearch Logstash Kibana* (ELK *Stack*)	Muhamad Nur Arifin, Sugiartowo, Emi Susilowati	2018	*Log Event Management Server* menggunakan ELK Stack untuk membaca dan menganalisis log *services* pada server *CentOS7* dan *Ubuntu* 14	Semua log *services* SSH yang terjadi pada *server client* dapat dikirimkan secara realtime ke *server* utama ELK *Stack*	Kinerja monitoring berfokus pada service ssh menggunakan ELK *Stack*, seperti percobaan kesalahan login ssh.	Perlunya monitoring lebih lanjut pada service dan log lainnya.	Menggunakan SIEM untuk monitoring dari serangan *Denial of Service*, *Port Scanning*, dan *Bruteforce Attack*.

No	Judul	Oleh	Tahun	General Ide	Hasil	Kelebihan	Kelemahan	Perbandingan
3	*Log Event Management Server* Menggunakan *Elastic Search Logstash Kibana* (ELK *Stack*)	Walidatus h Sholihah,	2020	Log event management server menggunakan ELK *Stack* yang dapat mempermudah dalam membaca dan menganalisis log pada server dengan OS *centos* 7.	Pengujian memasukkan *username* dan *password* yang salah secara berulang, hasil semua kegagalan dan keberhasilan dapat ditampilkan oleh *Kibana*	Menggunakan ELK *Stack* dengan OS *centos* 7 sebagai *Log Event Management Serve*r. Pengujian dilakukan percobaan *login* dan *Bruteforce Attack*	Perlunya monitoring lebih lanjut pada service dan log lainnya.	Menggunakan SIEM *Splunk* sebagai perbandingan monitoring log pada SIEM Ubuntu Server. Pengujian berupa *Denial of Service*, dan *Port Scanning*

No	Judul	Oleh	Tahun	General Ide	Hasil	Kelebihan	Kelemahan	Perbandingan
4	Implementasi *Security Information and Event Management* (SIEM) dengan *Splunk* untuk Analisis Tren Ancaman Siber pada Jaringan UII.	Muhammad Rijal Kamal	2022	Analisis pada *log firewall* dengan mengimplementasikan SIEM Splunk sebagai solusi untuk menganalisis tren ancaman siber yang ada pada UII	*Threat* yang sering masuk ke jaringan UII sebanyak 3.511.236 events, hasil dari *rules vulnerability* sebanyak 2.162.260 events, hasil dari rules *severity* menampilkan 1.223.811 level *critical*	*Log firewall* yang digunakan adalah *log Palo Alto Network*. Hasil dari jumlah ancaman dan serangan diimplementasikan dengan SIEM splunk berupa grafik yang dapat ditampilkan dan dibaca di dashboard	Simulasi serangan dan deteksi belum secara real-time untuk membandingkan performa dan hasil yang didapat. Tidak menerapkan *rules* pencarian pada *Splunk*.	Simulasi serangan menggunakan Kali Linux sebagai Attacker dan SIEM *Elastic Stack* sebagai perbandingan monitoring log. Parameter Pengujian serangan berupa *Denial of Service*, dan *Port Scanning*

No	Judul	Oleh	Tahun	General Ide	Hasil	Kelebihan	Kelemahan	Perbandingan
5	Analisa *Security Information and Event Management* (SIEM) Menggunakan *Elastic Stack* SIEM dan *Splunk*	Muhammad Alfandi	2022	Implementasi *Elastic Stack* SIEM dan *Splunk* dalam merekam dan mengumpulkan *log* dari serangan *Fingerprinting, SQL Injection, Denial of Service* (DoS) dan *Port Scanning.*	*Elastic Stack* dan *Splunk* berhasil mendeteksi semua serangan yang terjadi selama 3 hari pengujian. Dengan hasil deteksi serangan yang memiliki persamaan dan perbedaan.	Pengujian dilakukan dengan serangan *Fingerprinting*, *SQL Injection*, DoS dan *Port Scanning*. Dapat mengirimkan notifikasi semua serangan yang terjadi melalui email ke *administrator.*	*Elastic Stack* tidak berhasil mengirimkan notifikasi email ke *administrator*. Parameter pengujian hanya untuk membaca dan menganalisa log.	Parameter pengujian berupa kecepatan ingest *log*, deteksi serangan, dan penggunaan *resource* komputer.

2.3 Jaringan Komputer

Jaringan Komputer adalah kumpulan komputer ataupun perangkat dan peralatan lainnya yang saling terhubung. Data dan informasi ditransmisikan melalui kabel ataupun nirkabel, memungkinkan pengguna jaringan komputer untuk bertukar data dan sumberdaya. Setiap komputer, printer atau perangkat lainnya yang terhubung ke jaringan disebut *node* dan sebuah jaringan komputer bisa memiliki dua, puluhan bahkan jutaan *node* yang saling terhubung. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya dan setiap bagian dari jaringan komputer dapat meminta atau memberikan layanan. Pihak yang meminta layanan disebut klien dan yang memberikan layanan disebut *server*.

2.4 Keamanan Jaringan

Keamanan jaringan adalah praktik untuk melindungi sistem dan jaringan dari serangan siber, kerusakan, dan akses yang tidak sah. Hal ini mencakup penggunaan teknologi, kebijakan, dan prosedur untuk memastikan bahwa informasi dan sumber daya jaringan terlindungi dari ancaman dan risiko yang muncul dari serangan siber dan kegiatan berbahaya lainnya (Purba & Efendi, 2021).

Tujuan utama dari keamanan jaringan adalah untuk melindungi informasi sensitif dan sumber daya jaringan dari akses yang tidak sah dan kerusakan yang disebabkan oleh serangan siber, seperti *virus*, *worm*, *trojan*, dan *spyware*. Untuk mencapai tujuan ini, keamanan jaringan melibatkan sejumlah teknologi, termasuk SIEM, *firewall*, IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System*), VPN (*Virtual Private Network*), dan enkripsi (Kaur, Tejvir Malhotra, Vimmi Singh, 2014).

Selain teknologi, keamanan jaringan juga melibatkan kebijakan dan prosedur yang dirancang untuk memastikan bahwa pengguna mematuhi standar keamanan dan menjaga informasi sensitif terlindungi. Beberapa contoh tindakan yang dapat dilakukan untuk meningkatkan keamanan jaringan adalah, memperkuat kata sandi, memperbarui dan memantau sistem keamanan secara teratur, membatasi akses ke informasi sensitif, serta memberikan pelatihan keamanan bagi karyawan dan pengguna. Dengan meningkatnya serangan siber yang terjadi, penting untuk memprioritaskan keamanan jaringan untuk melindungi informasi sensitif dan sumber daya jaringan dari ancaman siber.

Gambar 2.1 CIA Triad

Terdapat tiga aspek, elemen atau tujuan utama dari keamanan komputer yang disebut dengan CIA Triad. CIA Triad tersebut terdiri dari *Confidentiality*, *Integrity* dan *Availability* (Samonas & Coss, 2021). Adapun tiga elemen dari CIA Triad yaitu :

1) *Confidentiality* (Kerahasiaan): Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Aspek ini berkaitan dengan

perlindungan informasi dari akses yang tidak sah atau tidak diizinkan oleh pihak yang tidak berwenang

2) *Integrity* (Integritas): Menjamin bahwa informasi tetap utuh dan tidak diubah tanpa izin atau kebutuhan. Aspek ini menjamin bahwa informasi tetap terjaga keasliannya dan tidak dirubah, baik secara tidak sengaja maupun disengaja.

3) *Availability* (Ketersediaan): Menjamin bahwa informasi dapat diakses oleh pihak yang berwenang kapanpun dibutuhkan. Aspek ini berkaitan dengan ketersediaan informasi, jadi informasi harus tersedia dan dapat diakses saat dibutuhkan

2.5 *Security Information and Event Management* (SIEM)

Gambar 2.2 SIEM

SIEM (*Security Information and Event Management*) adalah sebuah solusi teknologi yang digunakan untuk mengumpulkan, mengelola, menganalisis, dan memberikan laporan informasi keamanan dari berbagai sumber data di dalam organisasi. SIEM dapat memantau dan menganalisis aktivitas jaringan dan sistem untuk mendeteksi serangan siber, kejadian yang mencurigakan atau aneh, dan

kelemahan keamanan lainnya. SIEM dapat mengintegrasikan data dari berbagai sumber, termasuk *log*, perangkat jaringan, sensor keamanan, aplikasi, sistem operasi, dan perangkat lainnya, dan kemudian melakukan analisis terhadap data tersebut.

Dalam praktiknya, SIEM biasanya dilengkapi dengan fitur seperti pemantauan keamanan *real-time*, deteksi ancaman siber, manajemen kejadian keamanan, dan pelaporan keamanan. Dengan menggunakan SIEM, organisasi dapat meningkatkan tingkat keamanan informasi mereka dan meningkatkan kesiapan mereka dalam menghadapi ancaman keamanan yang ada atau yang potensial. SIEM sering digunakan oleh organisasi besar dan kompleks, termasuk pemerintah, perusahaan keuangan, dan industri kritis seperti energi dan kesehatan. SIEM juga menjadi bagian penting dari berbagai standar keamanan, seperti ISO/IEC 27001 dan NIST *Cybersecurity Framework* (Williams, 2016).

2.6 Splunk

Gambar 2.3 *Splunk*

Splunk adalah sebuah platform analisis data dan pengelolaan log yang digunakan untuk mengumpulkan, menganalisis, dan mengelola data dari berbagai sumber, termasuk sistem, aplikasi, dan jaringan. *Splunk* dapat digunakan untuk mengumpulkan data dari berbagai sumber seperti *log file*, jaringan, *database*, dan

sistem operasi, dan kemudian menganalisis dan memvisualisasikan data tersebut dalam bentuk grafik, tabel, dan *dashboard* (Abidian, 2021).

Dalam konteks keamanan informasi, *Splunk* dapat digunakan sebagai platform SIEM (*Security Information and Event Management*) untuk membantu organisasi mendeteksi serangan siber dan kejadian keamanan lainnya pada sistem mereka. *Splunk* juga dapat membantu organisasi dalam menjaga kepatuhan peraturan, melacak aktivitas pengguna, serta melakukan analisis forensik jika terjadi insiden keamanan.

Selain itu, *Splunk* juga dapat digunakan untuk tujuan operasional, seperti pemantauan kinerja sistem, pengelolaan log, dan analisis data bisnis. Dengan kemampuan analisis dan visualisasi yang kuat, *Splunk* menjadi salah satu *platform* yang populer dan banyak digunakan di berbagai industri, termasuk teknologi, keuangan, kesehatan, dan pemerintahan.

2.7 Elastic Stack

Gambar 2.4 *Elastic Stack*

Elastic Stack adalah kumpulan perangkat lunak *open-source* yang digunakan untuk mengumpulkan, mengelola, dan menganalisis data dari berbagai

sumber, termasuk *log*, jaringan, dan aplikasi. *Elastic Stack* terdiri dari empat produk utama, yaitu:

1. *Elasticsearch*: mesin pencari dan analitik data yang digunakan untuk mencari, menganalisis, dan memvisualisasikan data dari berbagai sumber. *Elasticsearch* dapat melakukan pencarian teks dan analisis data dengan cepat dan efisien.
2. *Logstash*: alat pengumpul dan pengolahan *log* yang digunakan untuk mengumpulkan, mengolah, dan mentransformasi data dari berbagai sumber, termasuk *log file*, *syslog*, dan perangkat jaringan lainnya. *Logstash* juga dapat memperkaya data dan mengirimkannya ke berbagai tujuan, seperti *Elasticsearch*, *Kibana*, atau tujuan lainnya.
3. *Kibana*: antarmuka pengguna untuk data visualisasi dan analitik. *Kibana* dapat digunakan untuk membuat *dashboard*, grafik, dan laporan berdasarkan data dari *Elasticsearch*. *Kibana* memungkinkan pengguna untuk memvisualisasikan data dalam bentuk grafik, diagram, dan tampilan lainnya.
4. *Beats*: alat pengumpul data ringan yang digunakan untuk mengumpulkan data dari berbagai sumber, termasuk sistem operasi, aplikasi, jaringan, dan infrastruktur. *Beats* dapat mengirim data langsung ke *Elasticsearch* atau *Logstash* untuk diproses dan dianalisis.

Elastic Stack sering digunakan untuk tujuan *log management*, pemantauan kinerja aplikasi, analisis keamanan, dan pemrosesan data besar (Affandi, 2022). Dengan dukungan terhadap berbagai sumber data dan kemampuan analisis yang

kuat, *Elastic Stack* menjadi salah satu solusi terkemuka untuk pengelolaan dan analisis data.

2.8 Serangan Siber (*Cyber Attacks*)

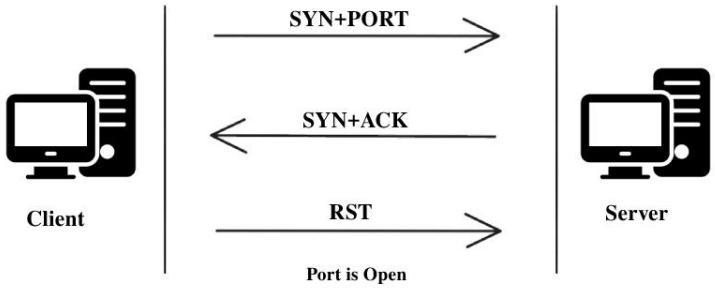
Cyber attacks merupakan serangan yang dilakukan melalui jaringan internet atau sistem komputer untuk mengakses, mengubah, atau menghapus informasi sensitif atau membahayakan sistem. Serangan ini dapat dilakukan melalui berbagai cara seperti *phishing*, *malware*, *ransomware*, *ddos attack*, dan lainnya (Bendovschi, 2015). Tujuannya biasanya untuk memperoleh keuntungan finansial, memperoleh informasi rahasia, atau merusak reputasi suatu organisasi atau individu. Serangan siber yang digunakan pada penelitian ini adalah *Port Scaning*, *Denial of Service* (DoS) *Attack* dan *Bruteforce Attack*.

2.8.1 Port Scanning

Port scanning adalah suatu teknik untuk mengidentifikasi port yang terbuka pada sistem atau jaringan komputer. *Port scanning* dilakukan dengan menggunakan perangkat lunak khusus yang mencoba menghubungi *port-port* tertentu pada sistem atau jaringan (Anif et al., 2015). *Port* adalah pintu masuk atau keluar dari suatu komputer atau jaringan yang digunakan untuk berkomunikasi dengan perangkat lain. Setiap *port* memiliki nomor yang unik dan spesifik. Dalam jaringan komputer, port digunakan untuk mengirim dan menerima informasi.

Dengan melakukan *port scanning*, seorang *attacker* atau penyerang dapat mengidentifikasi *port-port* yang terbuka pada sistem atau jaringan. Informasi ini dapat digunakan untuk mengeksploitasi sistem dan mendapatkan akses yang tidak

diizinkan ke dalam sistem atau jaringan. *Port scanning* dapat dilakukan secara manual dengan menggunakan *software* khusus atau otomatis seperti *nmap*.



Gambar 2.5 *Process of Port Scanning*

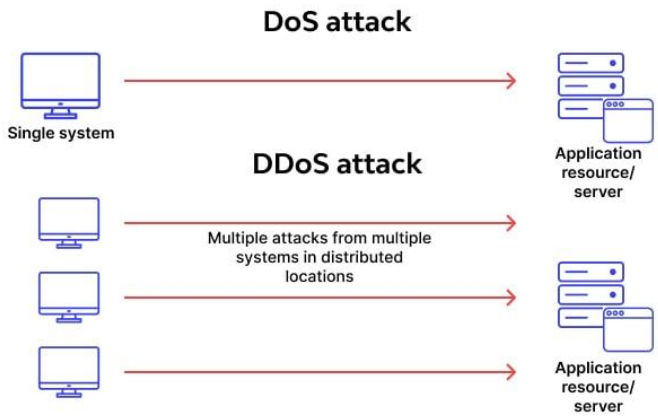
Port scanning dapat dilakukan oleh administrator jaringan untuk mengidentifikasi kerentanan atau celah keamanan dalam sistem atau jaringan mereka. Namun, *port scanning* juga dapat digunakan oleh penyerang untuk mencari celah keamanan yang dapat dimanfaatkan untuk melakukan serangan lebih lanjut. Oleh karena itu, penggunaan *port scanning* harus dilakukan dengan hati-hati dan hanya untuk tujuan yang sah.

2.8.2 *Denial of Service* (DoS) *Attack*

Denial of Service (DoS) *Attack* atau serangan DoS adalah serangan siber yang bertujuan untuk menghentikan atau memperlambat layanan atau aksesibilitas sistem atau jaringan dengan membanjiri sumber daya sistem atau jaringan dengan lalu lintas yang sangat tinggi (Bogdanoski et al., 2013).

Serangan DoS dilakukan dengan mengirimkan sejumlah besar permintaan atau lalu lintas yang berlebihan ke sistem atau jaringan sehingga tidak dapat

menangani lalu lintas yang datang dan menyebabkan layanan menjadi tidak tersedia bagi pengguna yang sah. Serangan DoS dapat dilakukan dengan berbagai cara, seperti membanjiri situs web dengan permintaan, mengirimkan email berlebihan ke server email, atau mengirimkan permintaan ping yang berlebihan ke sistem.



Gambar 2.6 *Process of Denial of Service* (DoS) *Attack*

Serangan DoS dapat merugikan suatu organisasi atau individu dengan mengganggu layanan dan menghambat bisnis atau operasi. DoS *Attack* juga dapat digunakan sebagai distraksi untuk mengalihkan perhatian dari serangan lain yang lebih berbahaya. Untuk melindungi sistem dan jaringan dari serangan DoS, organisasi dan individu dapat mengadopsi berbagai tindakan seperti memperkuat keamanan jaringan, membatasi jumlah permintaan yang dapat diterima, dan menggunakan teknologi pengamanan seperti SIEM.

2.8.3 *Bruteforce Attack*

Bruteforce attack atau serangan *bruteforce* adalah teknik serangan siber yang digunakan untuk memecahkan atau menebak kata sandi atau kunci enkripsi dengan mencoba semua kemungkinan kombinasi secara berturut-turut hingga menemukan kombinasi yang benar (Pratita, 2016). Serangan *bruteforce* dapat

dilakukan dengan menggunakan perangkat lunak khusus yang secara otomatis mencoba semua kombinasi yang mungkin untuk kata sandi atau kunci enkripsi pada suatu sistem atau jaringan. Serangan ini dilakukan dengan mengirimkan sejumlah besar permintaan ke sistem atau jaringan dalam waktu yang sangat singkat.

Gambar 2.7 *Process of Bruteforce Attack*

Serangan *bruteforce* biasanya dilakukan pada kata sandi atau kunci enkripsi yang lemah atau mudah ditebak, seperti kata sandi yang terdiri dari kombinasi sederhana atau terlalu pendek. Namun, serangan *bruteforce* juga dapat dilakukan pada kata sandi yang kuat dengan menebak secara acak seluruh kemungkinan kombinasi, yang memerlukan waktu dan sumber daya yang cukup besar. Serangan *bruteforce* dapat digunakan untuk mengambil alih akun pengguna, mengakses data yang sensitif atau rahasia, dan melakukan aktivitas ilegal lainnya. Untuk melindungi sistem dan jaringan dari serangan *bruteforce*, organisasi dan individu dapat mengadopsi berbagai tindakan seperti menggunakan kata sandi yang kuat, membatasi jumlah upaya *login* yang dapat dilakukan, dan menggunakan teknologi pengamanan.

2.9 VMware Workstation

VMware adalah perusahaan teknologi informasi yang berfokus pada pengembangan solusi virtualisasi dan *cloud computing*. *VMware* dikenal sebagai pengembang dan penyedia produk-produk virtualisasi yang dapat memungkinkan beberapa sistem operasi berjalan di atas satu mesin fisik.

Gambar 2.8 VMware

Produk utama *VMware* adalah *VMware vSphere*, sebuah platform infrastruktur virtualisasi yang memungkinkan pengguna untuk mengelola dan menjalankan mesin virtual dalam satu tempat yang terpusat. Selain itu, *VMware* juga menyediakan berbagai produk lain, seperti *VMware Fusion* untuk macOS, *VMware Workstation* untuk *Windows* dan *Linux*, serta produk untuk *cloud computing* dan manajemen jaringan. *VMware* banyak digunakan oleh perusahaan besar dan institusi akademis untuk meningkatkan efisiensi pengelolaan infrastruktur TI dan menghemat biaya. Solusi virtualisasi dari *VMware* memungkinkan pengguna untuk mengoptimalkan pemanfaatan sumber daya hardware, meningkatkan ketersediaan aplikasi dan layanan, serta meningkatkan keamanan dan stabilitas sistem.

2.10 Kali Linux

Kali Linux adalah sebuah sistem operasi yang dirancang khusus untuk digunakan dalam pengujian keamanan dan forensik digital. *Kali Linux* dikembangkan oleh *Offensive Security* dan berbasis pada sistem operasi *Debian*. *Kali Linux* dilengkapi dengan banyak perangkat lunak keamanan dan forensik digital, termasuk alat-alat untuk melakukan *penetration testing* (*pen-testing*), analisis jaringan, pemantauan keamanan, pemulihan data, dan lain-lain (Cisar & Pinter, 2019). Dalam *Kali Linux*, terdapat lebih dari 600 alat-alat keamanan dan forensik digital yang tersedia untuk digunakan.

Gambar 2.9 *Kali Linux*

Kali Linux sangat berguna bagi para profesional keamanan, *administrator* sistem, dan pengembang yang ingin melakukan pengujian keamanan dan forensik digital dalam lingkungan yang terkendali. Dalam *Kali Linux*, pengguna dapat melakukan berbagai jenis tes keamanan seperti *penetration testing*, *web application testing*, *wireless security testing*, dan masih banyak lagi. Namun, penting untuk dicatat bahwa *Kali Linux* harus digunakan secara etis dan hanya untuk tujuan legal seperti *pen-testing* dalam lingkup yang disetujui oleh organisasi yang bersangkutan.

Semua tes keamanan harus dilakukan dengan izin dan persetujuan pemilik sistem atau perangkat yang akan diuji.

2.11 Web Server

Web server adalah sebuah perangkat lunak atau program yang berfungsi untuk mengelola permintaan HTTP (*Hypertext Transfer Protocol*) dari klien atau pengguna internet. *Web server* bertindak sebagai jembatan antara browser pengguna dan aplikasi atau data yang terletak di server. Ketika seseorang mengakses suatu halaman web, *browser* mengirim permintaan HTTP ke server yang dijalankan oleh *web server*, kemudian *web server* akan memproses permintaan tersebut dan mengirimkan kembali respon berupa halaman web yang diminta oleh pengguna. Beberapa contoh *web server* populer adalah *Apache*, *Nginx*, dan *Microsoft* IIS.

2.12 Ubuntu Server

Ubuntu Server adalah sistem operasi yang didesain khusus untuk digunakan pada *server*. *Ubuntu* sendiri adalah salah satu distro *Linux* yang sangat populer, dan *Ubuntu Server* merupakan versi dari *Ubuntu* yang ditujukan untuk digunakan pada *server*, baik itu untuk *web server*, *file server*, *mail server*, dan lain-lain.

Gambar 2.10 *Ubuntu Server*

Ubuntu Server menyediakan banyak fitur dan kemampuan untuk mengelola *server*, termasuk dukungan untuk instalasi dan konfigurasi mudah melalui antarmuka baris perintah atau GUI (*Graphical User Interface*), manajemen paket, sistem keamanan yang kuat, serta dukungan untuk berbagai protokol jaringan seperti SSH (*Secure Shell*), FTP (*File Transfer Protocol*), dan lain-lain. *Ubuntu Server* juga dikembangkan dengan fokus pada stabilitas dan keamanan, sehingga sangat cocok untuk digunakan pada lingkungan *server* yang memerlukan keamanan dan ketersediaan data yang tinggi.

2.13 Risk Management

Risk management atau manajemen risiko adalah proses identifikasi, evaluasi, dan pengendalian risiko dalam sebuah organisasi atau kegiatan untuk mengurangi dampak potensial yang dapat terjadi. Tujuan utama dari manajemen risiko adalah untuk mengurangi risiko menjadi tingkat yang dapat diterima oleh organisasi. Proses manajemen risiko melibatkan beberapa tahapan, yaitu identifikasi risiko, penilaian risiko, pengembangan strategi pengendalian risiko, implementasi strategi pengendalian risiko, dan pemantauan dan evaluasi risiko. Dalam setiap tahapannya, manajemen risiko memerlukan analisis dan pemahaman yang mendalam tentang berbagai risiko yang mungkin terjadi, baik yang bersifat internal maupun eksternal (Wagiu et al., 2019).

Manajemen risiko penting dalam bisnis dan organisasi karena dapat membantu mengidentifikasi potensi kerugian atau dampak negatif yang mungkin terjadi pada bisnis atau kegiatan yang sedang dilakukan. Dengan manajemen risiko yang baik, organisasi dapat merencanakan dan mempersiapkan diri untuk

menghadapi risiko yang muncul dan mengambil tindakan yang tepat untuk mengurangi atau menghindari dampak negatif tersebut.

2.14 Risk Assessment

Risk assessment atau penilaian risiko adalah proses identifikasi, analisis, dan penilaian risiko dalam sebuah aktivitas atau organisasi untuk mengevaluasi kemungkinan terjadinya dampak negatif dan mengukur tingkat risiko yang terkait dengan aktivitas atau organisasi tersebut.

Proses penilaian risiko biasanya melibatkan empat tahapan yaitu:

1. Identifikasi risiko: Tahap ini melibatkan mengidentifikasi dan mendefinisikan potensi risiko yang mungkin terjadi pada organisasi atau aktivitas tertentu.
2. Analisis risiko: Tahap ini melibatkan analisis mendalam tentang sumber risiko dan kemungkinan terjadinya dampak negatif yang terkait dengan risiko tersebut.
3. Penilaian risiko: Tahap ini melibatkan penilaian atau pengukuran risiko yang terkait dengan aktivitas atau organisasi tertentu.
4. Pemantauan dan evaluasi risiko: Tahap ini melibatkan pemantauan dan evaluasi risiko secara berkala untuk memastikan bahwa tindakan yang diperlukan telah diambil untuk mengurangi atau menghilangkan risiko tersebut.

Penilaian risiko sangat penting dalam manajemen risiko karena dapat membantu organisasi dalam memahami risiko yang terkait dengan aktivitas atau organisasi tertentu dan memutuskan tindakan apa yang harus diambil untuk

mengurangi atau mengelola risiko tersebut. Dengan melakukan penilaian risiko secara teratur, organisasi dapat meningkatkan keselamatan dan keamanan kegiatan mereka serta menghindari kerugian yang mungkin terjadi.

2.15 Metode Penelitian

Metode penelitian eksperimen adalah salah satu metode penelitian yang digunakan untuk menguji hipotesis atau teori dengan memanipulasi variabel bebas dan mengamati perubahan pada variabel terikat dalam suatu kondisi yang terkendali. Dalam metode penelitian eksperimen, peneliti memilih satu atau lebih kelompok subjek, mengendalikan faktor-faktor yang dapat mempengaruhi hasil penelitian, dan melakukan manipulasi variabel bebas untuk mengamati efeknya terhadap variabel terikat. Metode ini biasanya melibatkan pengukuran dan analisis statistik untuk menentukan apakah perbedaan antara kelompok-kelompok itu signifikan atau hanya kebetulan (Jaedun, 2011).

Tujuan dari metode penelitian eksperimen adalah untuk mengetahui sebab-akibat dalam suatu fenomena dan memperoleh data yang dapat dipertanggungjawabkan secara ilmiah. Metode ini sering digunakan dalam berbagai bidang seperti psikologi, ilmu sosial, biologi, dan fisika.

2.16 Metode Pengujian

Pada pengujian terdapat metode yang digunakan untuk menganalisis hasil dari pengujian kinerja *Splunk* dan *Elastic Stack* dalam mendeteksi serangan *Denial of Service* (DoS) *Attack*, *Port Scanning*, dan *Bruteforce Attack*. Metode *Mean* atau rata-rata melibatkan menjumlahkan semua nilai yang diuji dan membaginya dengan jumlah total nilai tersebut. Ini adalah metode paling umum dan sederhana untuk

mencari nilai rata-rata. Metode inilah yang akan digunakan untuk menganalisa hasil pengujian berdasarkan kecepatan *ingest log*, deteksi *alert* serangan, waktu notifikasi *alert* dan penggunaan *resource* dari kedua SIEM tersebut.