Jurnal Ismetek *ISSN 2406-9841*
Vol. 20 No.1 Desember Tahun 2025 *e-IISN 2986-2973*

ANALISIS DAN IMPLEMENTASI LOG UNTUK DETEKSI SERANGAN WEB PADA ORGANISASI

Sigit Wibisono
Program Studi Teknik Inforatika,FTI, Institut Teknologi Budi Utomo Jakarta
wsigitwibisono@gmail.com

Abstrak
Adanya jejaring komputer pertukaran data dan informasi saat ini adalah begitu sangat mudah. Pada suatu organisasi atau institusi menggunakan sistem informasi berbasis Web adalah pilihan yang tepat. Sistem informasi berbasis Web ini dimaksudkan adalah agar suatu organisasi atau institusi dapat dengan mudah dikenal pihak lain, atau sebagai media publikasi. Namun dalam perkembangnnya muncul tantangan yaitu berupa gangguan, bahkan ancaman. Gangguan atau ancaman tersebut bisa dari dalam dan dari luar organisasi atau institusi. Pada kasus ini akan dibuat log pemantauan organisasi dalam satu dasbor pada server internal, terutama dengan menggunakan elasticsearch untuk merekam aktivitas yang terjadi. Setiap server keamanan memiliki file log sistem, yang berfungsi untuk merekam aktivitas yang terjadi pada server. Secara tradisional suatu organisasi telah mempertimbangkan untuk lebih berkonsentrasi pada mitigasi, yang terkait erat satu sama lain dalam mengumpulkan informasi dan data, untuk mendeteksi ancaman pengguna dari dalam Dasar untuk membangun kemampuan manajemen log server dalam organisasi, terutama server, seperti berapa lama setiap jenis data log server harus disimpan, jenis peristiwa yang harus dicatat.
Kata kunci : Elasticsearch, Log File, Data Log, Server,
.

1. PENDAHULUAN

Jejaring komputer memungkinkan pengguna memiliki peran penting dalam pertukaran data dan informasi. Sejumlah data dan informasi yang memiliki nilai arti tinggi, akan terkirim dengan mudahnya. Sistem informasi berbasis Web saat ini menjadi salah satu pilihan yang ada pada Dinas Komunikasi, Informatika dan Statistik Pemerintah Provinsi DKI Jakarta khusunya Bidang Siber dan Sandi. Sebuah organisasi atau institusi. Sistem informasi berbasis Web dapat digunakan sebagai media publikasinya. Namun dengan adanya peningkatan teknologi jejaring komputer pada Sistem Informasi, dalam perkembangannya menumbuhkan ancaman atau gangguan dari berbagai pihak, baik dari dalam maupun dari luar.

Sistem ini konsentrasi pada mengidentifikasi pengguna yaitu orang dalam yang akan bertindak sehingga menimbulkan potensi resiko yang membahayakan Secara tradisional suatu organisasi telah mempertimbangkan untuk lebih berkonsentrasi pada mitigasi, yang terkait erat satu sama lain dalam mengumpulkan informasi dan data, untuk mendeteksi ancaman pengguna dari dalam. Setiap server keamanan memiliki file log sistem, yang berfungsi untuk merekam aktivitas yang terjadi pada server. Pada kasus ini akan dibuat log pemantauan organisasi dalam satu dasbor pada server internal, terutama dengan menggunakan elasticsearch untuk merekam aktivitas yang terjadi. Selanjutnya ditampilkan pemberitahuan yang diterima melalui email tentang aktivitas server secara real time.

Terdapat tiga elemen konsentrasi utama yaitu menetapkan Aturan Kebijakan. Organisasi harus menetapkan kebijakan untuk memantau log server dengan tujuan untuk mengurangi risiko. Dasar untuk membangun kemampuan manajemen log server dalam organisasi, terutama server, seperti berapa lama setiap jenis data log server harus disimpan, jenis peristiwa yang harus dicatat. Perspektif Terpusat Tambahkan aturan baru di SIEM untuk mendeteksi temuan peristiwa log server yang mencurigakan dari analisis log server dan dengan cepat menampilkan gaya data eksklusif dalam satu dasbor. Temukan insiden di log analisis server Data log dapat ditinjau untuk mendeteksi kejadian yang tidak biasa.

2. METODOLOGI

Pada sub bab ini ditampilkan beberapa metode seperti Elasticsearch, Log File serta Deteksi Serangan.

2.1 Elasticsearch

Elasticsearch adalah aplikasi open source dibuat menggunakan bahasa pemrograman Java yang berfungsi sebagai alat pencarian, penyimpanan dan analisis log, dibangun berdasarkan konsep kerja sistem pencarian Apache Lucene. Elasticsearch merupakan databases berbasis documented oriented storage atau NoSQL database. Metode penyimpanan berorientasi dokumen ini sangat berbeda jauh dengan metode tradisional, yaitu table oriented storage seperti database MySQL dan Oracle, NoSQL database menyimpan data dalam bentuk format JSON (JavaScript Object Notation) document. Pencarian data dengan NoSQL sangat luar biasa cepat disebabkan setiap field terindeks secara otomatis. Elasticsearch compatible dengan berbeagai macam sistem operasi seperti Linux dan Windows. (Haditya et al., n.d.).

2.2 Log Files

Pada sub bab Log Files ini meliputi Log Overview, Log Collection, Log Visualization, serta Log Anaysis.

2.2.1 Log Overview

Gagasan tentang manusia yang membaca log pada mesin individual adalah sesuatu yang anakhronisme. Pendekatan ini dengan cepat menjadi tidak terkendali ketika banyak layanan dan server terlibat. Tujuan log dengan cepat menjadi masukan untuk kueri dan grafik untuk memahami perilaku di banyak mesin, sesuatu yang ditulis dalam bahasa Inggris file hampir tidak sesuai untuk jenis log terstruktur. (Kreps, 2015)

2.2.2 Log Collection

Perangkat keamanan atau server akan merekam log yang kemudian dikumpulkan secara real time yang digunakan oleh analis dalam aktivitas monitoring keamanan jaringan mereka. Meningkatnya kebutuhan untuk upgrade sistem akan mendorong ukuran log untuk terus meningkat. Model data mining sering diadopsi untuk mengetahui prilaku sistem informasi. Namun, sebelum memasuki fase ini, log perlu diurai karena format log yang tidak terstruktur, sehingga dapat diubah menjadi informasi yang dapat dipelajari oleh analis untuk peningkatan sistem di masa mendatang. (Kreps, 2015)

2.2.3 Log Visualization

Sistem visualisasi insiden keamanan digunakan untuk membantu dalam analisis layanan atau informasi tentang protokol yaitu TCP dan UDP, serta menampilkan insiden keamanan yang diwakili oleh simbol dalam visualisasi berbasis matriks. Tingkat resiko serangan juga ditandakan oleh beberapa warna, visualisasi lain juga menggunakan diagram batang untuk menampilkan jenis alarm, tanda alarm, tingkat resiko dan kategori aplikasi dan layanan. (Zhang & Zhao, 2013)

Saat ini kibana juga digunakan oleh banyak organisasi sebagai dasbor analisis visual, dengan adanya analisis visual mempercepat analisis dan proses respon dalam menangani masalah keamanan informasi.

2.2.4 Log Analysis

Analisis log dan kejadian saling berhubungan satu sama lain dalam kumpulan informasi dalam mendeteksi ancaman. Untuk analisis log korelasi event atau peristiwa diperlukan agar menyaring data yang tidak diinginkan dan mengeksekusi satu atau lebih tindakan (Ambre & Shekokar, 2015). Membangun aturan dan paket. Hanya paket TCP, UDP, dan ICMP yang secara acak dihasilkan oleh sumber paket untuk mensimulasikan jaringan yang sebenarnya. Lima atribut digunakan dalam paket yaitu protokol, IP sumber, port sumber, IP tujuan dan port tujuan.Aturan penyaringan untuk paket TCP, UDP, dan ICMP memiliki persentase yang berbeda karena:karakteristik lalu lintas jaringan yang sebenarnya. TCP adalah 70%, UDP adalah 10% dan akun ICMP untuk 20%. Rentang nilai setiap atribut dihasilkan secara acak (Zhang & Zhao, 2013)

Tabel. 1 Atribut Analis Paket

Protocol	Source IP	Source Port	Destination IP	Destination Port
TCP	202.80.169.29	100	129.110.96.64	80
UDP	202.80.169.64	225	129.110.96.64	443
ICMP	202.80.169.65	389	129.110.96.64	445

(Sumber : Dokumen Penelitian)

Penjelasan tentang metode penelitian yang digunakan dalam penelitian. Dapat dibuatkan dalam diagram alir.

2.3 Deteksi Serangan

Pada Sub Bab ini berisi Tinjauan Deteksi Intrusi, Analisis Deteksi Intrusi, yang diuraikan pada Sub-Sub Bab berikut.

2.3.1 Tinjauan Deteksi Intrusi

Dalam beberapa tahun terakhir, jumlah orang yang menggunakan internet telah meningkat dengan cepat, yang hal ini menunjukkan bahwa persyaratan untuk sistem proteksi yang sesuai. Maka secara umum, bahwa gangguan berbahaya atau serangan terhadap komputer dan database informasi dapat merusak atau mengganggu keamanan komputer berupa kebijakan yang harus diperhatikan, yaitu, Kerahasiaan, Integritas dan Ketersediaan (CIA). Karena luas penggunaan internet, jaringan komputer sangat rentan terhadap kebocoran informasi yang memberikan kontribusi pada munculnya Sistem Deteksi Intrusi (IDS) (Hajisalem & Babaie, 2018).

2.3.2 Analisis Deteksi Intrusi

Volume kalkulasi tinggi dan perubahan terus-menerus dalam distribusi data jaringan telah membuatnya lebih sulit untuk menganalisis data dan mendeteksi perilaku abnormal. Solusi data besar telah menjadi esensial. Anomali yang teridentifikasi dapat memberikan keluaran yang dapat digunakan untuk memahami perilaku jaringan, membedakan serangan, memberikan yang lebih baik keamanan siber, dan melindungi infrastruktur penting. Hasilnya divisualisasikan setelah pengurangan dimensi menggunakan Principal Component Analysis (PCA) Analisis perlu dilakukan pada file log karena file log memantau adalah alat berharga yang menyediakan informasi tentang kemungkinan aktivitas jahat (Ambre & Shekokar, 2015).

3. HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan dibahas Gambaran Analisis Sistem, Analisis Kebutuhan Hardware, Analisis Kebutuhan Software, Perancangan Sistem serta Pengujian Sistem

3.1 Gambaran Analisis Sistem

Analisis Sistem adalah bagaimana gambaran sistem yang akan dibangun atau akan diusulkan, termasuk dalam hal adalah perangkat keras serta perangkat lunak. Sehingga diharapkan sistem akan berjalan sesuai seperti apa yang diharapkn.

3.2 Analisis Kebutuhan Hardware

Pada percobaan sistem menggunakan perangkat keras dengan spesifikasi seperti termuat pada tabel 3.1

Tabel 2. Spesifikasi Perangkat Keras

Perangkat Keras	Spesifikasi dan Deskripsi
Host Setup	1 TB RAM, 134.35GHz and 30 TB Storage Per node (4 nodes) 256 GB RAM and 16 core Intel(R) Xeon(R) Silver 4208 CPU @ 2.1 GHz
Virtual Machine Setup	40 GB RAM, 5.1TB DISK and 16 vCPU Untuk menjalankan OS

(Sumber : Dokumen Penelitian)

Seperti pada tabel 3.1 di atas, seluruh sistem elastic membutuhkan ruang memori atau RAM karena digunakan sebagai analisis sistem.

3.3 Analisis Kebutuhan Software

Spesifikasi perangkat lunak atau software yang dibutuf adalah sebagai berikut tersebut pada tabel 3.

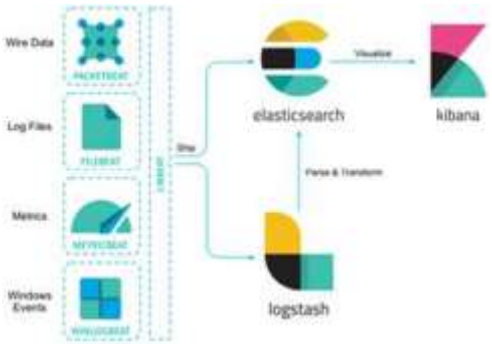
Tabel 3. Spesifikasi Perangkat Lunak

Perangkat Lunak	Spesifikasi dan Deskripsi
Host Setup	Nutanix Acropolis AHV
Virtual Machine Setup	Ubuntu 20.04.1 LTS (Focal Fossa)
Analysis Platform	Elastic 7.9.3 (cluster)
Endpoint Detection and Response	Elastic Agent 7.16.2

(Sumber : Dokumen Penelitian)

3.4 Perancangan Sistem

Pada tahap **p**erancangan system, secara umum dilakukan dengan maksud untuk memberikan gambaran umum tentang sistem yang baru atau sistem yang akan diusulkan. Dalam penelitian ini, melakukan perancangan arsitektur sistem yang terdiri dari masing-masing menggunakan sistem operasi Linux Ubuntu 20.04.1 LTS (Focal Fossa).



Gambar.1 Perancangan Sistem
(Sumber : Dokumen Penelitian)

Perancangan sistem ini merupakan gambaran keseluruhan dari proses analisis secara fisik yang akan dijalankan. Dalam perancangan ini, digambarkan suatu sistem dengan tampilan yang real dalam mengimplementasikannya

3.5 Pengujian Sistem

Pengujian ini akan memaparkan pengujian yang peneliti lakukan setelah pengimplementasian ELK Stack. Pada penelitian telah dilakukan Pengujian Efektivitas dan Pengujian Analyzer Log serta Lalu lintas Jaringan berbasis ELK Stack.

3.5.1 Pengumpulan Log

Dari hasil pengumpulan log pada perangkat keamanan jaringan, perlu diusulkan pada bagian sebelumnya, telah ditemukan beberapa aktivitas yang mencurigakan yang dimungkinkan akan mengganggu keamanan perangkat tidak dapat mendeteksi, yang kemudian akan dianalisis, evaluasi, dan validasi. Penulis membuat tabel berisi ancaman yang tidak diketahui yang penulis dapatkan selama penelitian ini.

Tabel 4.Daftar Aktivitas yang Mencurigakan

No	Protocol	Data Source
1	SSH	Firewall
2	SMB	EDR

(Sumber : Dokumen Penelitian)

3.5.2 Analisis

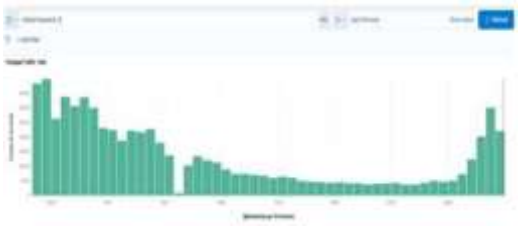
Pada tahap analisis, penulis membuat hipotesis tentang pencarian ancaman dengan menyaring log yang telah dikumpulkan untuk mendapatkan informasi yang berguna untuk analisis lebih lanjut, kemudian penulis membuat tabel dari kasus yang ditemukan, untuk analisis, evaluasi dan validasi.

Tabel 5. Analisis Daftar Mencurigakan

No	Protocol	Events	Data Source
1	SSH	Percobaan Login	EDR
2	SMB	Permintaan koneksi ke file sharing	EDR

(Sumber : Dokumen Penelitian)

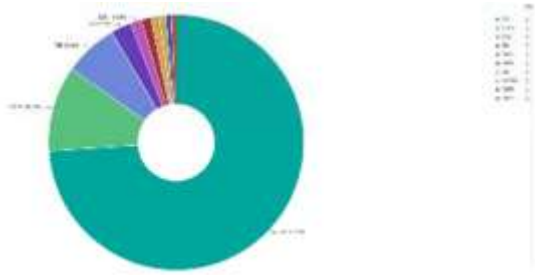
3.5.3 Analisis SSH



Gambar 2 Analisis lalu lintas filter *Firewall*
(Sumber : Dokumen Penelitian)

Pada gambar grafik 3.2 diatas merupakan hasil dari proses analisa dengan memfilter allow traffic gambar dan alamat IP tujuan untuk melihat apakah lalu lintas itu benar-benar aman atau ada beberapa lalu lintas berbahaya yang membutuhkan analisis lebih

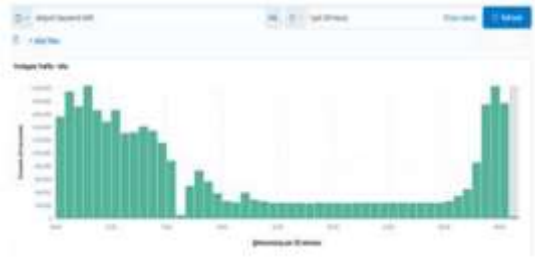
lanjut. Terlihat pada grafik menunjukkan lonjakan lalu lintas dan perlu dilakukan kajian dan analisis yang mendalam.



Gambar 2. Port 22 10 lalu lintas teratas dari lalu lintas yang diizinkan
(Sumber : Dokumen Penelitian)

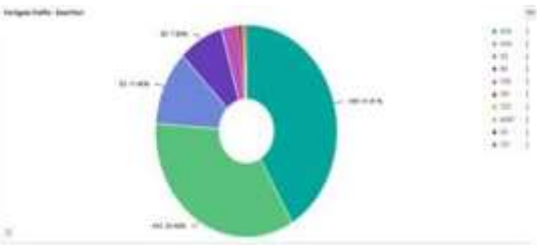
Dari gambar 3.3, dapat dilihat tindakan yang diizinkan pada port 22 menjadi kategori 10 port teratas yang banyak digunakan, dan dalam penelitian ini melakukan analisis pada port 22.

3.5.4 Analisis SMB



Gambar 3 Analisa lalu lintas filter *Firewall*
(Sumber : Dokumen Penelitian)

Pada gambar grafik 3.4 diatas merupakan hasil dari proses analisis dengan memfilter *allow traffic* gambar dan alamat IP tujuan untuk melihat apakah lalu lintas yang benar-benar aman atau ada beberapa lalu lintas berbahaya yang membutuhkan analisis lebih lanjut. Terlihat pada grafik menunjukkan lonjakan lalu lintas dan perlu dilakukan kajian dan analisis yang mendalam.



Gambar 4 Port 445 lalu lintas teratas dari
(Sumber : Dokumen Penelitian)

Pada gambar 3.5, dapat terlihat tindakan yang diizinkan pada port 445 menjadi kategori 10 port teratas yang banyak digunakan, dan dalam penelitian ini melakukan analisis pada port 445.

3.5.5 Evaluasi SSH

Gambar .5 Jumlah kegagalan percobaan login
(Sumber : Dokumen Penelitian)

Dari gambar 3.6 Terdeteksi adanya percobaan login dan terdapat alamat IP yang mengirimkan paket pada protokol 22 ke banyak alamat ip, dengan jumlah kegagalan login sebanyak 788 kali. Terdeteksi 3 host server yang terdampak bruteforce atau percobaan login dari 3 source IP Address, seperti gambar 3.7 berikut ini.

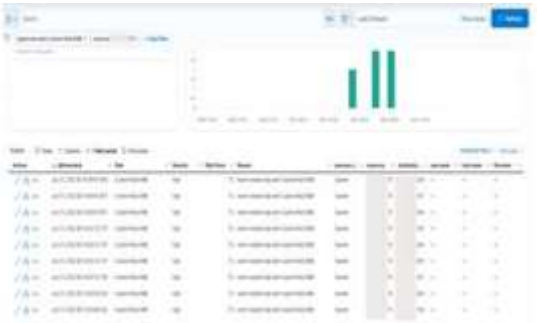
Gambar 6 Host server yang terbuka
(Sumber : Dokumen Penelitian)

Evaluasi pada protokol SSH didasarkan pada log yang di dapatkan dari EDR, seperti yang terlihat pada Gambar 3.8 terlihat bahwa terdapat alamat IP yang mengirimkan paket pada protokol 22 ke banyak alamat ip dengan waktu periodik yang sangat sering. sehingga, EDR menganggap ini sebagai lalu lintas tidak normal, jadi status di trafic EDR diberi label sebagai waspada atau anomali.

Gambar .7 Protokol SSH dengan port 22
(Sumber : Dokumen Penelitian)

3.5.6 Evaluasi SMB

Evaluasi pada protokol SMB/NFS didasarkan pada log yang didapatkan dari EDR, seperti yang terlihat pada Gambar 3.9 terlihat bahwa terdapat alamat IP yang mengirimkan paket pada protokol 445 ke banyak alama ip dengan waktu periodik yang sangat sering. Namun, EDR masih menganggap ini sebagai lalu lintas normal, jadi status di trafic EDR belum diberi label sebagai waspada atau anomali.



Gambar 8 Protokol SMB de ngan port 445

(Sumber : Dokumen Penelitian)

Dari data yang didapatkan yaitu pada gambar 3.9, melalui visualisasi pada evaluasi Protokol SMB, adalah menunjukkan bahwa sebuah host membuat permintaan dengan protokol SMB pada port 445 tanpa pemilik host menyadarinya, yang berarti ada layanan yang secara otomatis membuat permintaan ke SMB.

3.5.7 Validasi SSH

Pada saat melakukan validasi menggunakan pendekatan forensik jaringan, untuk menentukan aktivitas jahat pada host korban. Alat yang digunakan adalah Wireshark sebagai alat forensic jaringan yang di lakukan dalam kasus ini.

Gambar 3.10 TCP Dump untuk memrikas koneksi paket data port 22
(Sumber : Dokumen Penelitian)

Setelah dilakukan evaluasi dengan forensik jaringan untuk mendapatkan informasi yang lebih akurat, dapat dilihat pada Gambar 3.10 hal ini dapat dilihat pada alamat IP yang SYN beberapa alamat IP lain menggunakan port 22.

Gambar 11 Visualisasi Elasticsearch
(Sumber : Dokumen Penelitian)

Pada gambar 3.11 setelah dilakukan validasi lebih lanjut dengan elasticsearch untuk melihat file service yang di gunakan. Dalam proses evaluasi pemeriksaan koneksi port, diberikan label PID 183134 sebagai hydra digunakan dan sehingga dapat dilihat PID 183114 memiliki lalu lintas keluar pada alamat IP x.x.x.114 dengan port 22

5. KESIMPULAN

Setelah melalui beberapa tahap melakukan pengumpulan, analisis, evaluasi,

dan validasi dari keamanan jaringan log peristiwa perangkat untuk menemukan anomali dan aktivitas mencurigakan. validasi hasilnya, penulis telah berhasil mendeteksi 1 aktivitas jahat dari 2 yang mencurigakan kegiatan dan telah divalidasi. setelah mendeteksi ancaman yang tidak diketahui dengan membuat aturan baru untuk memblokirnya dengan benar untuk lalu lintas masuk di masa mendatang

DAFTAR PUSTAKA

[1] Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, *45*(C), 436–445. https://doi.org/10.1016/j.procs.2015.03.175

[2] Haditya, P., Program, P., Multimedia, S. T., & Jaringan, D. (n.d.). *Implementasi log management server menggunakan ELK (Elasticsearch, Logstash dan Kibana) Stack pada server web snort di Pt.XYZ.*

[3] Hajisalem, V., & Babaie, S. (2018). A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. *Computer Networks*, *136*, 37–50. https://doi.org/10.1016/j.comnet.2018.02.028

[4] Hassan, W. U., Bates, A., & Marino, D. (2020). Tactical provenance analysis for endpoint detection and response systems. Proceedings - IEEE Symposium on Security and Privacy, 2020-May, 1172–1189. https://doi.org/10.1109/SP40000.2020.00096

[5] Kreps, Jay. (2015). *I logs : event data, stream processing, and data integration*. O'Reilly Media.

[6] Zhang, J., & Zhao, Y. (2013). A user term visualization analysis based on a social question and answer log. *Information Processing and Management*, *49*(5), 1019–1048. https://doi.org/10.1016/j.ipm.2013.04.003

.