ISSN 1412-2782 eISSN 2407-9103
Vol 22. No. 1 Januari 2023

Jurnal
POLI-TEKNOLOGI

Implementasi Intrusion Detection System (Ids) Suricata Dan Management Log Elk Stack Untuk Pendeteksian Kegiatan Mining

Ayu Rosyida Zain ✉, Prihatin Oktivasari, Nur Fauzi Soelaiman, Faiz Watsiqul Umam
Program Studi Teknik Multimedia dan Jaringan, Politeknik Negeri Jakarta, Depok Indonesia 16425.
✉e-mail :ayu.rosyidazain@tik.pnj.ac.id

Abstrak

IDS (Intrusion Detection System) merupakan salah satu metode keamanan jaringan komputer yang ingin melindung komputer dalam sebuah jaringan. Pada penelitian ini dibuat implementasi sistem IDS menggunakan Suricata dan management log ELK Stack. Dimana Suricata merupakan salah satu IDS engine yang mempunyai kelebihan lebih mudah dalam konfigurasi rules dan management log ELK Stack dapat mempermudah dalam monitoring keamanan jaringan. Pengujian dan analisis dilakukan terhadap implementasi sistem IDS Suricata dan management log ELK Stack, meliputi Funcional Test, Response Time, Detection Rate, dan memory usage akibat kegiatan web mining. Suricata berhasil mendeteksi terhadap serangan dan juga kegiatan web mining serta menampilkannya pada interface berbasis Web ELK Stack.

Article History
Submitted: 02/10/2022
Revised : 09/01/2023
Accepted : 31/01/2023
Published: 31/01/2023

Kata Kuncis:
IDS, Suricata, ELK Stack, Mining

Pendahuluan

IDS (Intrusion Detection System) adalah proses monitoring yang digunakan untuk mendeteksi dan menganalisa aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Intrusion Detection System memiliki sistem kerja atau mesin analisis (analysis engine) dalam mendeteksi setiap aktvitas-aktivitas serangan yang ada, secara umum analysis engine ini dapat di kategorikan menjadi dua yaitu : Signature-Based Detection dan Anomaly/Statistical Detection. Management log adalah salah satu komponen yang penting dalam melakukan normalisasi data, hal ini dikarenakan banyak aktivitas yang melibatkan dalam proses analisis log seperti mengumpulkan, filter, dan memvisualisasikan data. Selain itu, management log berguna dalam pengambilan suatu keputusan yang efisien dan efektif. Pada penelitian ini, dirancang suatu sistem keamanan berbasis IDS (Intrusion Detection System) dengan menggunakan software open source yaitu Suricata dan pembuatan management log menggunakan ELK Stack. Sistem ini akan berfungsi sebagai sehingga administrator bisa melakukan pengawasan dan juga bertindak dengan cepat untuk mengatasi serangan. Dengan implementasi sistem ini diharapkan administrator dapat melakukan terhadap suatu server secara efektif dan efisien.

Dasar Teori

A. Intrusion Detection System (IDS)

IDS merupakan perangkat keras atau lunak yang digunakan untuk memonitoring aktifitas jaringan yang dapat merusak atau melanggar aturan dan melaporkan nya. IDS mempunyai tiga fugsi yaitu monitoring, mendeteksi dan menghasilkan alert). Intrusion adalah aktivitas tidak sah atau tidak diinginkan yang dapat mengganggu konfidensialitas, integritas dan ketersediaan dari informasi yang terdapat di sebuah sistem. IDS akan mengawasi lalu lintas data pada sebuah jaringan atau mengambil data dari berkas log [1], [2] .

B. Suricata

Suricata adalah perangkat lunak pendeteksi dan pencegahan intrusi (Intrusion setection and preventation system) open source yang merupakan generasi berikutnya dari perangkat-perangkat IDS/IPS yang ada saat ini. Suricata adalah sebuah aplikasi yang berbasis IDS/IPS yang melakukan deteksi terhadap serangan atau gangguan dengan metode signature based dengan mengeluarkan *alert* apabila terdapat paket yang dianggap jenis serangan oleh

rules yang dimiliki oleh Suricata. Selanjutnya paket serangan akan di tindak lanjuti oleh *administrator* untuk melakukan pencegahan [3]

C. ELK Stack

Elasticsearch, Logstash dan Kibana adalah tool yang berguna untuk mengumpulkan log dan juga menvisualisasi suatau data. Elasticsearch berguna untuk menyimpan semua log yang berasal dari server, Logstash merupakan sebuah perangkat lunak open source untuk mengumpulkan dan memfilter log dan juga membuat index untuk log kemudian di simpan pada Elasticsearch. Kibana adalah web interface yang berguna untuk menampilkan log baik dalam bentuk grafik maupun visualisasi lainnya. Filebeat berguna untuk mengirim log dari setiap server kepada Logstash [4] .

D. Port Scanning

Port Scanning adalah aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah mesin. Port adalah sebuah pintu, maka scanning adalah proses untuk mengamati atau meninjau. Pada intinya, melakukan port scanning ialah untuk mengidentifikasi port-port apa saja yang terbuka, dan mengenali OS target [5].

E. Denial of Service (Dos) Attack

DoS *Attack (Denial Of Service Attack)* adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber daya (*resource*) yang dimiliki oleh suatu komputer. Serangan DDOS dilakukan menggunakan banyak komputer atau virtual komputer untuk menyerang satu target, penyerangan dilakukan secara bersamaan tanpa melihat jarak dan waktu [6]

F. Mining

Mining adalah aktivitas penambangan mata uang yang dilakukan pencatatan sistem transaksi dari satu atau dua mata uang kripto yang kemudian dikirim ke penyimpanan dalam format blok informasi. Proses mining dilakukan dalam sebuah tempat yang bernama farm (dilakukan oleh farmer), sedangkan penambangan (miner) menerima nilai kompensasni pada mata uang kripto. Teknologi *cryptocurrency* merupakan dasar dari bitcoin yang memungkinkan untuk terciptanya sebuah sistem terintegrasi yang mampu saling bertukar mata uang dalam satu jaringan *peer-to-peer* [7].

G. Wireshark

Wireshark merupakan tool yang bertujuan untuk menganalisis paket data serangan. Wireshark juga melakukan pengawasan paket secara real time dan kemudian menangkap paket dan menampilkannya secara lengkap. Wireshark memiliki seperangkat fitur yakni tersedia untuk sistem operasi linux dan windows, menangkap paket data dari antarmuka jaringan, Wireshark juga dapat menangkap lalu lintas dari banyak jenis media jaringan yang berbeda [8].

H. Detection Rate

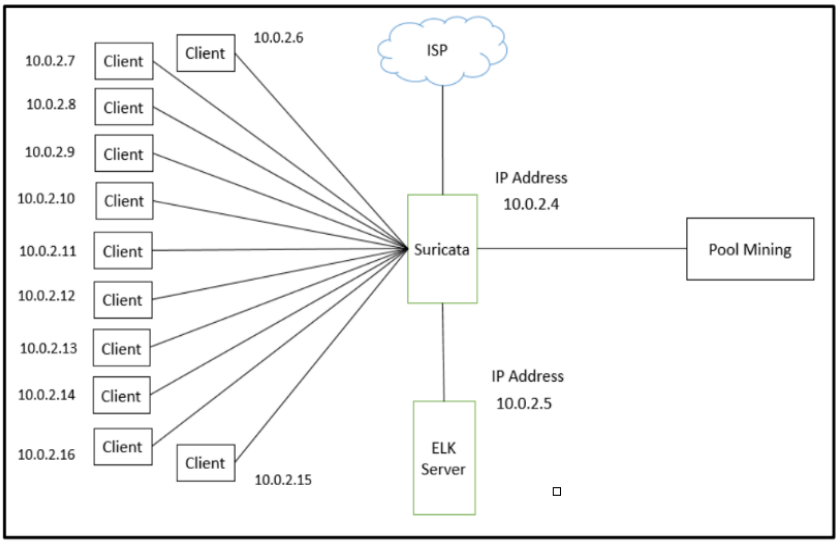
Detection rate dilakukan untuk mengukur Suricata selaku IDS dalam mendeteksi serangan *web mining* atau disebut juga *detection rate*. Untuk mencari besar *detection rate* dari IDS Suricata digunakan metode *matrix confusion* untuk mengolah hasil deteksi setiap *web mining* yang telah diuji. *Confusion matrix* merupakan metode alat ukur berbentuk *matrix* untuk mencari ketepatan dalam suatu pengklasifikasian data. Pada *table confusion matrix* setiap baris merepresentasikan *actual class*, sedangkan setiap kolom merepresentasikan *predicted class* [9].

ISSN 1412-2782 eISSN 2407-9103
Vol 22. No. 1 Januari 2023

Metode Penelitian

Jaringan system menggunakan beberapa perangkat seperti server dan pc. Pada metode penelitian ini akan dijelaskan mengenai gambaran sistem, analisis kebutuhan sistem dan kebutuhan perangkat.

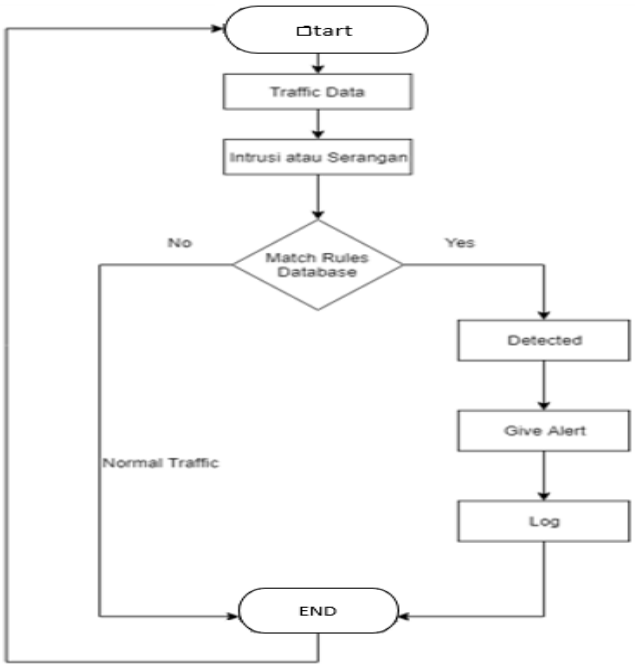
A. Gambaran Sistem



Gambar 1. Struktur Sistem

IDS Suricata akan diimplementasikan pada OS Linux yang juga terdapat DNS dan Web Server sebagai layanan yang diberikan. Suricata dipasang pada OS Debian 9 sedangkan untuk *ELK Stack* pada os ubuntun 18.04. *ELK Stack* dibangun untuk membuat Kibana web interface dimana dapat melakukan visualisasi data sehingga mempermudah Administrator dalam melakukan pengawasan jaringan.

B. Analisis Kebutuhan Sistem



Gambar 2. Alur Sistem

Intrusion Detection System (IDS) server membutuhkan beberapa aplikasi dan program yang digunakan. Suricata digunakan untuk mendeteksi adanya serangan yang terjadi dan hasil notifikasi tersebut tersimpan dalam bentuk log. Untuk memvisualisasikan log tersebut dibutuhkan ELK Stack dimana Elasticsearch berperan sebagai database sedangnkan Logstash sebagai filter terhadap log dan terakhir yaitu kibana untuk menapilkan data via web-based. Kemudian melakukan instllasi filebeat pada server Suricata untuk membawa data dalam fast.log.

C. Kebutuhan Perangkat

1. Kebutuhan perangkat keras

Tabel 1. Kebutuhan Perangkat Keras

No.	Nama	Spesifikasi	Deskripsi
1.	Server Sruicata	Debian9 (64-bit) memori 1024MB	Perangkat yang digunakan sebagai server Suricata
2.	Server ELK Stack	Ubuntu 18.04 (64-bit) Memori 4000MB	Perangkat yang digunakan sebagai server ELK Stack untuk visualisasi data
3.	PC Attacker	Kalilinux2.6 (64-bit) Memori 1024MB	Perangkat untuk melakukkan percobaan attack.
4.	PC Client	Debian9 (64-bit) Memori 1024	Perangkat untuk melakukan kegiatan web mining.

2. Kebutuhan perangkat lunak

Tabel 2. Kebutuhan Perangkat Lunak

No.	Nama	Deskripsi
1.	Linux Dash (Ubunu,debian, dan kalilinux)	Perangkat lunak yang digunakan untuk melihat performansi dan perbandingan performansi server
2.	Suricata	Perangkat lunak yang digunakan untuk membuat DNS dari alamat IP dan menampilkan *web interface.*
3.	ELK Stack	Perangkat lunak yang digunakan untuk melakukan *port scanning* pada server target.
4.	Hping3	Perangkat lunak yang digunakan untuk melakukan serangan sistem.
5.	Nmap	Perangkat lunak yang digunakan untuk melakukan eksploitasi pada server target.
6.	Wireshark	Perangkat lunak yang digunakan untuk mengetahui response time pada attacker.

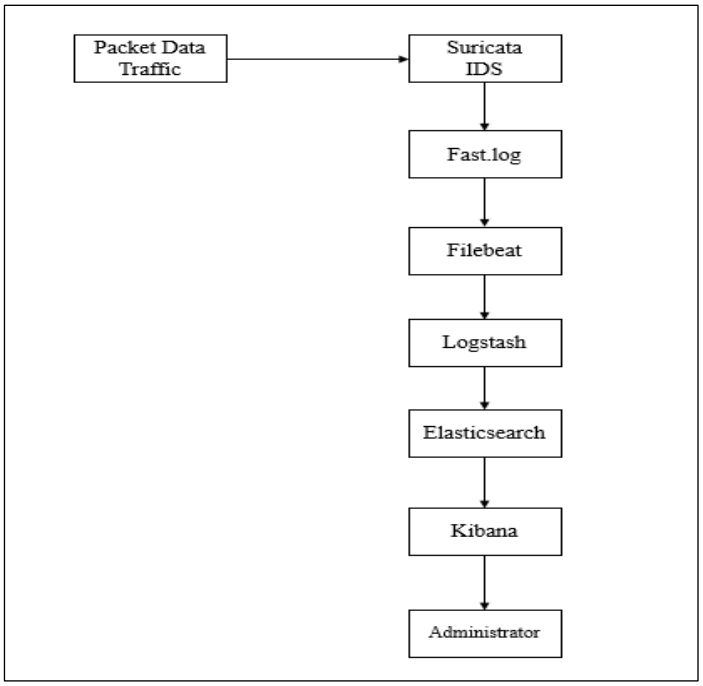
Hasil dan Pembahasan

Pada sub bab ini akan di bahas hasil analisis dari implementasi dan pengujian yang sudah dilakukan

A. Implementasi

Implementasi yang akan dilakukan pada penelitian ini adalah sebagai berikut：

ISSN 1412-2782 eISSN 2407-9103
Vol 22. No. 1 Januari 2023



Gambar 3. Alur Implementasi Sistem

Tabel 3. Kebutuhan Perangkat Lunak dalam Uji Sistem

No.	Nama	Deskripsi
1.	Debian Server	Sistem Operasi yang digunakan untuk Server IDS.
2.	Ubuntu Server	Sistem Management Log yang digunakan untuk Server ELK Stack.
3	Suricata	Perangkat lunak yang digunakan untuk mendeteksi serangan.
4	Kali Linux	Sistem Operasi yang digunakan untuk sebagai penyerang.
5.	Debian	Sistem Operasi yang digunakan untuk sebagai klien.

B. Pengujian

1. Pengujian *Port Scanning*
   a. Perintah yang dilakukan untuk *Port Scanning*

```
# nmap -sV 10.100.2.2
```

   b. Hasil log dari serangan yang dilakukan

```
06/29/2016-18:59:42.517259  [**] [1:2200025:1] ET SCAN posible Port Scanning [**
] [Classification: (null)] [Priority: 3] {ICMP} 10.100.2.10:8 -> 10.100.2.2:9
06/29/2016-18:59:42.517320  [**] [1:2200025:1] ET SCAN posible Port Scanning [**
] [Classification: (null)] [Priority: 3] {ICMP} 10.100.2.2:0 -> 10.100.2.10:9
```

Gambar 4. Log Serangan Port Scanning

2. Pengujian *Dos Attack*
   a. Perintah yang dilakukan untuk *Dos Attack*

```
# hping3 -c 10000 -d 120 -S -w
64 -p 21 --flood 10.100.2.2
```

ISSN 1412-2782 eISSN 2407-9103
Vol 22. No. 1 Januari 2023

b. Hasil log dari serangan yang dilakukan

```
06/18/2016-15:46:18.718027  [**] [1:2210045:2] ET DOS Large amount of TC
P [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {
TCP} 10.100.1.1:0 -> 10.100.1.10:9853
06/18/2016-15:46:18.718027  [**] [1:2210046:2] ET DOS Large amount of TC
P [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {
TCP} 10.100.1.1:0 -> 10.100.1.10:9853
```

Gambar 5. Log Serangan DoS Attack

3. Pengujian *Web Mining*

a. Perintah yang dilakukan untuk *Web Mining*

```
# Ping Poolto.be
```

b. Hasil log dari serangan yang dilakukan

```
06/18/2016-15:46:18.718027  [**] [1:2210045:2] ET DOS Large amount of TC
P [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {
TCP} 10.100.1.1:0 -> 10.100.1.10:9853
06/18/2016-15:46:18.718027  [**] [1:2210046:2] ET DOS Large amount of TC
P [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {
TCP} 10.100.1.1:0 -> 10.100.1.10:9853
```

Gambar 6. Log Serangan Web Mining

4. Pengujian ELK Stack

a. Hasil log dari serangan yang dilakukan

Gambar 7. Log Serangan ELK Stack

5. Analisis Hasil Pengujian

Berikut adalah analisis hasil pengujian

Tabel 4. Analisis Hasil Pengujian
Response Time

No	Jenis Serangan	Response Time	Hasil Pengujian
1	*Port Scanning*	0,0259211 detik	IDS Suricata berhasil mendeteksi
2	*DoS Attack*	0,3449451 detik	IDS Suricata berhasil mendeteksi
3	*Web Mining*	0,2739613 detik	IDS Suricata berhasil mendeteksi

Tabel 5. Confusion Matrix 30 web pengujian

		Predicted Class	
		Web Normal	Web Mining
Actual Class	Web Normal	True Negative(10)	False Positive(0)
	Web Mining	False Negative(0)	True Positive(20)

Penghitungan data *detection rate* dari Suricata menggunakan metode *confusion matrix* dalam mendeteksi kegiatan *web mining* dapat dilihat pada table 5.

- True Positive yaitu kondisi ketika Suricata menghasilkan peringatan (alert) berdasarkan pada identifikasi yang benar karena memang terjadi kegiatan web mining. (20)
- False Positive yaitu Suricata menghasilkan peringatan (alert) untuk sebuah kondisi yang sebenarnya tidak terdapat kegiatan web mining. (0)
- True Negative yaitu Suricata tidak menghasilkan peringatan (alert), karena memang tidak ada kegiatan web mining yang terjadi. (10)
- False Negative yaitu Suricata tidak menghasilkan peringatan (alert), tetapi kenyataannya telah terjadi kegiatan web mining pada sistem. (0)

Detection rate adalah rasio antara jumlah kegiatan web mining yang terdeteksi oleh IDS dengan jumlah kegiatan web mining yang dilakukan. Dengan Rumus sebagai berikut:

$$\mathrm{DR} = \frac{\mathrm{TruePositive}}{\#\mathrm{FalseNegative}+\#\mathrm{TruePositive}} \quad (1)$$

Dari rumus diatas diperoleh detection rate dari Suricata dengan pengujian 30 web adalah 1.00 atau 100%.

Tabel 6. Analisis Hasil Uji Memory Usage

No	JeJumlah klien	Memory usage
1	Satu	210.8 KIB
2	Lima	415.2 KIB
3	Sepuluh	460.4 KIB

Kesimpulan

Dengan adanya suricata sebagai IDS yang digunakan, setiap serangan yang ditujukan ke dalam jaringan akan dideteksi oleh suricata dengan pengecekan terhadap rules yang digunakan. Setiap serangan yang sudah masuk ke dalam database akan ditampilkan melalui web interface Kibana. Sehingga memudahkan administartor jaringan untuk melakukan pengecekan atau pengawasan terhadap jaringan.

Daftar Pustaka

[1] A. Sharifi, F. F. Zad, F. Farokhmanesh, A. Noorollahi, and J. Sharif, "An Overview of Intrusion Detection and Prevention Systems (IDPS) and Security Issues," *IOSR J Comput Eng*, vol. 16, no. 1, pp. 47–52, 2014, doi: 10.9790/0661-16114752.

[2] A. Sharifi, F. F. Zad, F. Farokhmanesh, A. Noorollahi, and J. Sharif, "An Overview of Intrusion Detection and Prevention Systems (IDPS) and Security Issues," *IOSR J Comput Eng*, vol. 16, no. 1, pp. 47–52, 2014, doi: 10.9790/0661-16114752.

[3] Prof. MA. A. P. Bilal Maqbool, "INTRUSION DETECTION AND PREVENTION SYSTEM: CLASSIFICATION AND REVIEW," *ARPN Journal of Science and Technology* , pp. 661–675, 2012.

[4] Harni Yusnidar and Jasni Mohamad, "VISUALIZING WEB SERVER LOGS INSIGHTS WITH ELASTIC STACK- A CASE STUDY OF UMMAIL'S ACCESS LOGS," *Malaysian Journal of Compuitng*, pp. 37–53, 2018.

[5] O. P. C. P. L. M. B. P. Eldow, "COMPUTER NETWORK SECURITY IDS TOOLS AND TECHNIQUES (SNORT/SURICATA)," *International Journal of Scientific and Research Publications,* pp. 593–597, 2016.

[6] S. Khadafi, B. D. Meilani, and S. Arifin, "SISTEM KEAMANAN OPEN CLOUD COMPUTING MENGGUNAKAN IDS (INTRUSION DETECTION SYSTEM) DAN IPS (INTRUSION PREVENTION SYSTEM)," *Jurnal IPTEK*, vol. 21, no. 2, p. 67, Dec. 2017, doi: 10.31284/j.iptek.2017.v21i2.207.

[7] A. S. S. T. , M. T. , P. S. T. , M. T. Sofyan Hadi, "Implementasi Network Intrusion Detection System pada Sistem Smart Identification," *e-Proceeding of Applied Science*, vol. 2, no. 3, pp. 1172–1176, Dec. 2016.

[8] D. Ankaa, *BITCOIN MINING DAN CRYPTOCURRENCY LAINNYA*. Jasakom : Jakarta, 2018.

[9] W. S. Yacob Hae, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, pp. 2095–2105, Dec. 2021.