Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 5, October 2023, pp. 1033-1039

DOI: https://doi.org/10.52436/1.jutif.2023.4.5.756
p-ISSN: 2723-3863
e-ISSN: 2723-3871

COMPARATIVE STUDY OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK DETECTION IN COMPUTER NETWORKS

Adam Zukhruf[*1], Bagus Fatkhurrozi[2], Andriyatna Agung Kurniawan[3]

[1,2,3]Electrical Engineering, Faculty of Engineering, Universitas Tidar, Indonesia
Email: [1]adamzukhruf54@gmail.com, [2]bagusf@untidar.ac.id, [3]andriyatna@untidar.ac.id

(Article received: Desember 14, 2022; Revision: Desember 28, 2022; published: October 15, 2023)

Abstract

Distributed Denial of Service (DDoS) attack is an internet crime that aims to consume server resources so that the server becomes unusable. Suricata, Snort and Wireshark are useful software applications for detecting DDoS attacks. This study aims to compare the performance of the snort, suricata and wireshark applications in detecting Distributed Denial of Service attacks. The comparison parameters used are the total attacks that can be detected and memory usage. The type of attack used in testing is syn flood and ping of death. The research results obtained by Suricata became the most effective application in this study compared to snort and wireshark. Suricata excels in memory usage in the two types of attacks performed with the percentage of memory usage being 0.1891 GB (4.975%) during syn flood attacks and 0.00114 GB (0.03%) during ping of death attacks. Suricata also excels in the percentage of the total number of detected ping of death attacks, namely 86,472%.

Keywords: *DDoS, performance comparison, ping of death, snort, suricata, wireshark.*

STUDI KOMPARASI EFEKTIVITAS PENDETEKSIAN SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA JARINGAN KOMPUTER

Abstrak

Distributed Denial of Service (DDoS) *attack* merupakan kejahatan internet yang memiliki tujuan untuk menghabiskan sumber daya dari *server* sehingga *server* menjadi tidak dapat digunakan. Suricata, Snort dan Wireshark merupakan aplikasi perangkat lunak yang berguna untuk mendeteksi serangan DDoS. Penelitian ini bertujuan untuk mengetahui perbandingan kinerja dari aplikasi snort, suricata dan wireshark dalam mendeteksi serangan *Distributed Denial of Service*. Parameter perbandingan yang digunakan adalah total serangan yang mampu terdeteksi dan penggunaan memori. Jenis serangan yang digunakan dalam pengujian adalah *syn flood* dan *ping of death.* Hasil penelitian yang telah didapatkan, Suricata menjadi aplikasi yang paling efektif dalam penelitian ini dibandingkan dengan snort dan wireshark. Suricata unggul penggunaan memori di dua jenis serangan yang dilakukan dengan persentase penggunaan memori adalah 0.1891 GB (4.975%) saat serangan *syn flood* dan 0.00114 GB (0.03%) saat serangan *ping of death*. Suricata juga unggul dalam persentase total jumlah serangan *ping of death* yang terdeteksi yaitu 86.472%.

Kata kunci: *DDoS, perbandingan kinerja, ping of death, snort, suricata, wireshark.*

1. PENDAHULUAN

Kejahatan *cyber* selalu berhubungan dengan penggunaan teknologi informasi dan komputer. Kejahatan *cyber* dilakukan dengan masuk ke dalam suatu sistem jaringan komputer secara tidak sah atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Serangan-serangan dan kejahatan internet sangat banyak ditemukan khususnya adalah serangan *Distributed Denial of Service* (DDoS). *Distributed Denial of Service* merupakan kejahatan internet yang memiliki tujuan yang negatif yaitu menghabiskan sumber daya dari *server* sehingga *server* tidak dapat digunakan.

Rabu 23 Februari 2022 terjadi serangan DDoS terhadap ukraina. Dilansir dari CNN Indonesia, Ukraina dilaporkan mengalami serangan siber DDoS yang diduga berasal dari Rusia. Serangan itu menyebabkan sejumlah bank dan situs pemerintah terdampak. Menurut peneliti dari perusahaan keamanan siber ESET, perangkat lunak berbahaya ini menyerang ratusan komputer di Ukraina. Otoritas Ukraina menyebut serangan ini bagian dari gelombang peretasan intensif yang menyasar negaranya [1]. Serangan DDoS juga terjadi di Indonesia. Pada pertengahan maret 2020, Liputan6 melaporkan situs resmi pemantauan virus corona

pemerintah provinsi Jakarta terkena serangan DDoS. Serangan ini mengakibatkan situs pemantauan virus corona sulit di akses bahkan tidak dapat di akses sama sekali oleh pengguna [2].

Keamanan jaringan komputer adalah masalah yang harus diperhatikan oleh setiap pengguna komputer[3]. Keamanan jaringan komputer merupakan bagian dalam suatu sistem yang sangat penting dalam menjaga validitas dan integritas data serta menjamin ketersediaan layanan pagi pengguna[4]. Sistem informasi pada jaringan komputer yang rentan mengakibatkan mudahnya penyusup (*intruder*) untuk masuk dan mengambil informasi rahasia pada sistem tersebut[5]. Oleh karena itu, perlu adanya sistem keamanan jaringan komputer untuk mencegah dan mengidentifikasi perilaku yang tidak sah dalam jaringan komputer, salah satunya serangan DDoS.

Serangan DDoS adalah jenis serangan berbahaya yang mengirimkan lalu lintas berbahaya ke *node* tertentu atau sejumlah besar *node* melalui sejumlah besar komputer yang berbeda, yang merupakan bagian dari sebuah sistem (*bot*) yang dikendalikan penyerang secara sah atau tidak. Hasil dari serangan semacam itu adalah sumber daya target kewalahan menangani paket yang tidak sah, dan tidak dapat secara efektif mengirimkan permintaan layanan yang sah[6]. Serangan ini sulit untuk dideteksi pada tahap awal karena merupakan jenis serangan kritis yang mengarahkan banyak node ke satu target sehingga dapat menyebabkan efek bencana pada korban dan mengganggu jaringan[7].

Distributed Denial of Service memiliki beberapa jenis serangan contohnya seperti *Syn flood* dan *ping of death*. *Syn flood* merupakan salah satu bentuk serangan DDoS yang memiliki tujuan untuk menghabiskan sumber daya dari *server* sehingga *server* menjadi terganggu dengan mengirimkan paket *syn* sebanyak-banyaknya dan akhirnya tidak dapat melayani lalu lintas jaringan yang sah[8]. Paket *syn* merupakan paket yang termasuk ke dalam protokol TCP yang berfungsi untuk membuat koneksi antar dua *host* dan dikirim oleh *host* yang ingin membuat koneksi[9]. *Transmission Control Protocol* (TCP) merupakan protokol yang berfungsi untuk proses tukar menukar data dari komputer satu ke komputer lain dalam jaringan internet[10].

Ping of death merupakan bentuk serangan dari DDoS yang dilakukan oleh penyerang menggunakan *tool* khusus terhadap target dengan mengirimkan *ping* dengan *size* yang tidak mampu diterima oleh komputer atau *server*[11]. Penyerang memanfaatkan protokol ICMP dalam melakukan serangan *ping of death* kepada target[12]. *Internet Control Message Protocol* (ICMP) merupakan protokol yang berfungsi untuk memberikan pesan *error* atau kesalahan dalam komputer[13]. *Distributed Denial of Service* mempunyai dampak negatif yaitu menurunnya kecepatan dan kinerja dari jaringan, *server* tidak dapat berfungsi sebagaimana mestinya, kerusakan sistem yang bersifat sementara bahkan permanen, kerugian finansial untuk biaya pemulihan *server* akibat serangannya.

Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusupan. Sistem Deteksi Penyusupan tidak melakukan pencegahan terjadinya penyusupan[14]. Beberapa aplikasi yang dapat digunakan untuk melakukan pendeteksian terhadap DDoS *attack* adalah aplikasi suricata, aplikasi snort dan aplikasi wireshark.

Wireshark adalah salah satu dari alat analisa jaringan yang biasa dipakai oleh seorang network administrator untuk melakukan pemecahan masalah yang ada dalam jaringan[15]. Snort merupakan sebuah alat yang berfungsi untuk mendeteksi sebuah intrusi atau serangan pada jaringan[16]. Suricata merupakan suatu sistem deteksi intrusi berbasis *open source* yang dikembangkan oleh *Open Information Security Foundation* (OISF)[17].

Aplikasi yang digunakan dalam penelitian ini merupakan aplikasi yang bersifat *open source* yang banyak digunakan. Oleh karena itu, aplikasi tersebut menjadi pilihan dari peneliti untuk melakukan penelitian efektivitas pendeteksian serangan *Syn flood* dan *ping of death*. Parameter-parameter yang digunakan dalam perbandingan efektivitas yaitu total jumlah serangan yang mampu terdeteksi dan penggunaan memori dari ketiga aplikasi yang digunakan. Penelitian mengenai efektivitas dalam mendeteksi serangan DDoS memiliki tujuan untuk mengetahui perbandingan kinerja dari aplikasi snort, suricata dan wireshark dalam mendeteksi serangan *syn flood* dan *ping of death*. Penelitian ini diharapkan dapat digunakan sebagai referensi dalam memilih aplikasi deteksi keamanan pada jaringan komputer.

2. METODE PENELITIAN

Untuk melakukan penelitian mengenai Studi komparasi keefektifan aplikasi snort, suricata dan wireshark dalam mendeteksi serangan *Distributed Denial of Service*. Dibutuhkan alat dan bahan, diagram alir penelitian, topologi perancangan dan skenario pengujian untuk mendukung jalannya penelitian.

2.1. Alat dan Bahan

Alat yang digunakan dalam penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Perangkat Keras

No	Nama	Spesifikasi
1	Processor	AMD Quad Core FX-9830P
2	RAM	16GB
3	Penyimpanan	SSD 256GB HDD 1TB
4	VGA	AMD Radeon R7 AMD RX 460
5	Screen	15.6 inch

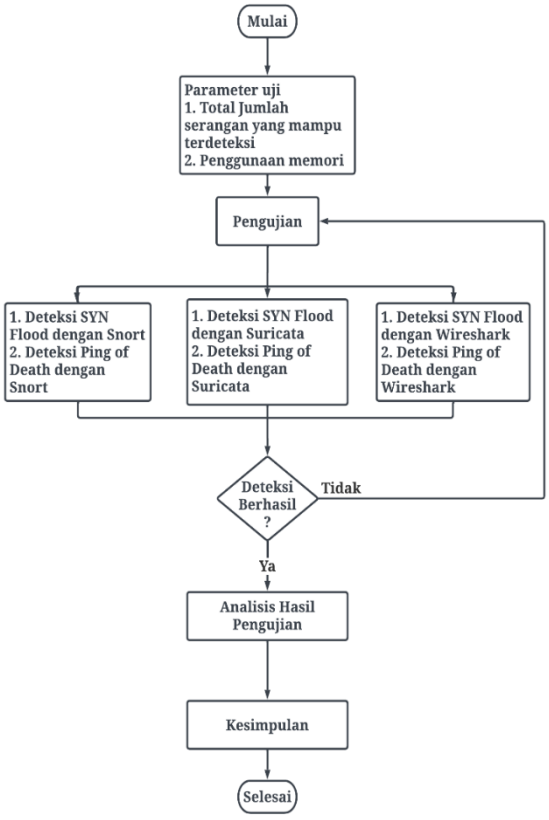
Bahan yang dibutuhkan dalam penelitian ini dapat dilihat pada Tabel 2.

Tabel 2. Perangkat Lunak

No	Nama	Spesifikasi	Keterangan
1	Oracle VM *Virtual box*	*Virtual box* versi 6.1	Berfungsi untuk menginstal ubuntu
2	Linux Ubuntu	Ubuntu versi 22.04	Berfungsi untuk penyerang dan *server*
3	Wireshark	Wireshark versi 3.4.4	Berfungsi untuk pendeteksian serangan DDoS
4	Snort	Snort versi 2.9.20	Berfungsi untuk pendeteksian serangan DDoS
5	Suricata	Suricata versi 6.0.6	Berfungsi untuk pendeteksian serangan DDoS
6	Hping3	Hping3 *for* ubuntu	Berfungsi untuk melakukan serangan

2.2. Diagram Alir Penelitian

Diagram alir yang ditunjukkan pada Gambar 1 digunakan untuk menggambarkan proses penelitian yang akan dibuat, agar penelitian dapat berjalan lebih terarah.

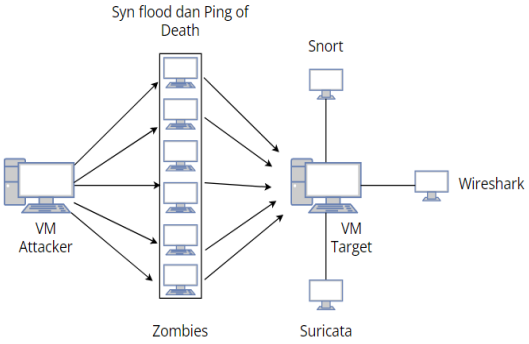


Gambar 1. Diagram Alir Penelitian

2.3. Topologi Perancangan

Topologi yang digunakan dalam penelitian ini ditunjukkan pada Gambar 2.

Serangan DDoS mencangkup sejumlah besar paket yang dikirim dari penyerang (*attacker*) menggunakan untuk melakukan penyerangan terhadap komputer server (target). Paket yang datang (*zombies*) merupakan paket yang sangat tinggi dan banyak jumlahnya sehingga membuat sumber daya dari korban atau target menjadi terkuras. *Attacker* menggunakan dua jenis serangan *Distributed Denial of Service* yaitu *Syn Flood* dan juga *Ping of death.* Masing-masing serangan dilakukan bergantian agar tidak terjadi crash saat pengujian.



Gambar 2. Topologi Perancangan

Dokumentasikan hasil dari pendeteksian masing-masing *software* dan juga melihat aktivitas perangkat keras yang digunakan saat mendapatkan serangan tersebut. Selanjutnya melakukan perbandingan keefektifan *software* dalam melakukan deteksi dari serangan DDoS sesuai dengan parameter yang sudah ditetapkan dengan melakukan analisa hasil pengujian dengan mencari standar deviasi, rata-rata serangan, rata-rata penggunaan memori dan persentase pendeteksian serangan.

$$Rata - rata = \sum \frac{x.}{n} \quad (1)$$

$$Standar\ Deviasi = \sqrt{\sum \frac{(X-(Rata-rata))^2}{n}} \quad (2)$$

$$Persentase\ Pendeteksian = \frac{sample\ serangan\ terdeteksi}{sample\ serangan\ terkirim} . 100 \quad (3)$$

Keterangan:
x = Nilai setiap sampel
n = Total sampel yang diambil

2.4. Skenario Pengujian

Penelitian ini menggunakan dua skenario pengujian. Langkah-langkah yang dilakukan dalam pengujian 1 sebagai berikut:

1) melakukan persiapan mengenai bahan-bahan yang akan digunakan dalam pengujian
2) melakukan pemasangan dan konfigurasi *virtual machine* pada windows, dengan mengatur spesifikasi yang akan digunakan masing-masing *virtual machine* sebagai berikut :
   a. 3.8 GB untuk RAM
   b. 2 inti *processor*
   c. 16 MB video *memory*
   d. 25 GB Penyimpanan

3) melakukan konfigurasi *virtual machine* untuk *server* dan *attacker* atau penyerang pada *virtual box*. Tahap ini dibuat satu *attacker* dan tiga buah untuk *server* dengan klasifikasinya sebagai berikut :
   a. Satu buah VM *server* untuk Snort
   b. Satu buah VM *server* untuk suricata
   c. Satu buah VM *server* untuk wireshark
4) melakukan konfigurasi jaringan agar VM *server* dan penyerang saling terhubung.
5) melakukan instalasi HPing 3 pada VM penyerang sebagai *tool* serangan *syn flood*.
6) melakukan serangan *syn flood* menggunakan Hping3 dari VM penyerang ke VM *server* Snort.
7) melakukan serangan *syn flood* menggunakan Hping3 dari VM penyerang ke VM *server* Suricata.
8) melakukan serangan *syn flood* menggunakan Hping3 dari VM penyerang ke VM *server* Wireshark.
9) melakukan pengambilan data hasil pengujian untuk dilakukan analisis sesuai parameter yang sudah ditetapkan.

Langkah-langkah yang dilakukan dalam pengujian 2 sebagai berikut:

1) melakukan persiapan mengenai bahan-bahan yang akan digunakan dalam pengujian
2) melakukan instalasi dan konfigurasi pada windows, dengan mengatur spesifikasi yang akan digunakan masing-masing *virtual machine* sebagai berikut :
   a. 3.8 GB untuk RAM
   b. 2 inti *processor*
   c. 16 MB video *memory*
   d. 25 GB Penyimpanan
3) melakukan konfigurasi *virtual machine* untuk *server* dan *attacker* atau penyerang dalam *virtual box*. Tahap ini dibuat satu *attacker* dan tiga buah untuk *server* dengan klasifikasinya sebagai berikut :
   a. Satu buah VM *server* untuk Snort
   b. Satu buah VM *server* untuk suricata
   c. Satu buah VM *server* untuk wireshark
4) melakukan konfigurasi jaringan agar VM *server* dan penyerang saling terhubung.
5) melakukan instalasi HPing 3 pada VM penyerang sebagai *tool* serangan *Ping of death*.
6) melakukan serangan *Ping of death* menggunakan Hping3 dari VM penyerang ke VM *server* Snort.
7) melakukan serangan *Ping of death* menggunakan Hping3 dari VM penyerang ke VM *server* Suricata.
8) melakukan serangan *Ping of death* menggunakan Hping3 dari VM penyerang ke VM *server* Wireshark.
9) melakukan pengambilan data hasil pengujian untuk dilakukan analisis sesuai parameter yang sudah ditetapkan.

3. HASIL DAN PEMBAHASAN

3.1. Penerapan Pengujian

Pada tahap ini, kegiatan yang dilakukan antara lain adalah instalasi aplikasi yang akan digunakan, konfigurasi antar aplikasi, pembuatan *rules*, simulasi percobaan serangan dan pendeteksian Snort.

Rules untuk mendeteksi serangan *syn flood* pada Snort sebagai berikut:

```
alert tcp $EXTERNAL_NET any->$HOME_NET any (msg: "Serangan Syn Flood!!"; detection_filter: track by_dst, count 800, seconds 1; sid:7679)
```

Rules untuk mendeteksi serangan *ping of death* pada Snort sebagai berikut:

```
alert icmp $EXTERNAL_NET any->$HOME_NET any (msg: "SERANGAN PING OF DEATH!!"; dsize:>1200; sid:479; rev:4;)
```

1) Suricata

Langkah-langkah yang dilakukan dalam pengujian 2 sebagai berikut:

Rules untuk mendeteksi serangan *syn flood* pada Suricata sebagai berikut:

```
alert tcp any any -> any 80 (msg: "Serangan Syn Flood"; flags: S; flow: stateless; threshold: type both, track by_dst, count 800, seconds 1; sid:2321; rev:1)
```

Rules untuk mendeteksi serangan *ping of death* pada Suricata sebagai berikut:

```
alert icmp any any -> any any (msg: "Ping of death Terdeteksi"; dsize:>1200; classtype:bad-unknown; sid:10001; rev:5;)
```

2) Wireshark

Wireshark tidak perlu membuat *rules* untuk mendeteksi serangan *syn flood* ataupun *ping of death*. Fitur yang dimiliki oleh wireshark memungkinkan wireshark untuk mendeteksi *Transmission Control Protocol* (TCP) dan *Internet Control Message Protocol* (ICMP) secara langsung dalam jaringan yang digunakannya.

3) *Attacker*

Perintah yang digunakan dalam melakukan serangan *syn flood* sebagai berikut:

```
hping3 –s –p 80 –flood ip target
```

Perintah yang digunakan untuk melakukan serangan *Ping of death* sebagai berikut:

```
hping3 –1 –d 67000 ip target - -flood
```

3.2. Hasil Pengujian

1) *Syn Flood*

Data hasil pengujian pendeteksian serangan *syn flood* yang telah dilakukan sebanyak 20 kali tiap aplikasi dan waktu pendeteksian serangan 1 menit tiap sampel didapatkan hasil yang disajikan dalam bentuk tabel terlihat pada tabel 3.

Tabel 3. Data Hasil Pengujian Serangan *syn flood*

	Snort				Suricata				Wireshark			
			Penggunaan Memori				Penggunaan Memori				Penggunaan Memori	
	Serangan	Terdeteksi	Pemakaian (GB)	Persentase (%)	Serangan	Terdeteksi	Pemakaian (GB)	Persentase (%)	Serangan	Terdeteksi	Pemakaian (GB)	Persentase (%)
1	1088935	1031219	0.3686	9.7	959786	923399	0.1900	5.0	981487	936564	2.3674	62.3
2	1124199	1038904	0.3686	9.7	923868	819584	0.1862	4.9	902568	866585	2.4130	63.5
3	1044953	1011795	0.3686	9.7	902270	818695	0.1900	5.0	994172	807765	2.2458	59.1
4	1114465	1080771	0.3686	9.7	901589	813590	0.1900	5.0	898346	876483	2.4434	64.3
5	1125047	1036459	0.3686	9.7	899777	810960	0.1900	5.0	885945	846561	2.3674	62.3
6	1104625	1024202	0.3648	9.6	895531	854003	0.1900	5.0	939965	806888	2.2344	58.8
7	1110827	1013207	0.3686	9.7	922924	913284	0.1862	4.9	883256	852099	2.3750	62.5
8	1091111	1008886	0.3686	9.7	844010	765935	0.1900	5.0	855838	849419	2.3560	62.0
9	1142345	1010488	0.3686	9.7	926764	911359	0.1900	5.0	877573	864734	2.4054	63.3
10	1104520	988846	0.3686	9.7	922938	879539	0.1900	5.0	887183	864462	2.4054	63.3
11	1095246	1032884	0.3648	9.6	924468	880059	0.1862	4.9	888107	869335	2.4168	63.6
12	1112006	1082433	0.3686	9.7	891561	788223	0.1900	5.0	882348	842931	2.3484	61.8
13	1094067	1024277	0.3686	9.7	924168	799906	0.1862	4.9	901045	850718	2.3674	62.3
14	1065617	1035308	0.3686	9.7	854006	805692	0.1900	5.0	937827	880835	2.4396	64.2
15	1074052	1008214	0.3686	9.7	908752	801002	0.1862	4.9	891153	871440	2.4244	63.8
16	1071325	1041855	0.3686	9.7	913095	839404	0.1900	5.0	906296	834209	2.3142	60.9
17	1108072	1030816	0.3686	9.7	900697	814510	0.1900	5.0	887441	885168	2.4624	64.8
18	1098926	1020081	0.3686	9.7	962224	892275	0.1900	5.0	910724	895031	2.4928	65.6
19	1054433	1001089	0.3686	9.7	921681	851994	0.1900	5.0	916541	874268	2.4320	64.0
20	1076329	983495	0.3686	9.7	915343	882745	0.1900	5.0	1065132	846253	2.3522	61.9

2) *Ping of death*

Data hasil pengujian yang telah dilakukan dalam pendeteksian serangan *ping of death* yang telah dilakukan sebanyak 20 kali tiap aplikasi dan dengan estimasi waktu pendeteksian serangan 1 menit terlihat pada tabel 4.

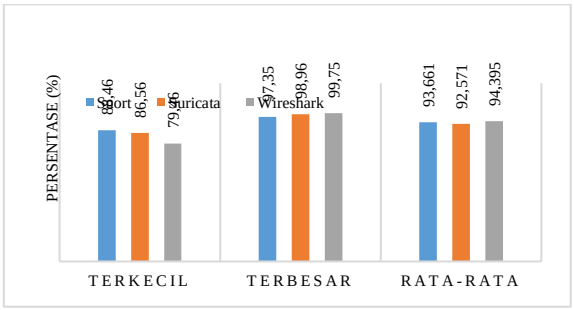
Tabel 4. Data Hasil Pengujian Serangan Ping of death

No	Snort				Suricata				Wireshark			
			Penggunaan Memori				Penggunaan Memori				Penggunaan Memori	
	Serangan	Terdeteksi	Pemakaian (GB)	Persentase (%)	Serangan	Terdeteksi	Pemakaian (GB)	Persentase (%)	Serangan	Terdeteksi	Pemakaian (GB)	Persentase (%)
1	1012702	486424	0.1596	4.20	901355	818301	0.0076	0.20	852813	633244	0.6650	17.50
2	977314	429729	0.1482	3.90	917851	844803	0.0000	0.00	964330	572959	0.5814	15.30
3	1016044	470024	0.1482	3.90	910915	821584	0.0038	0.10	872433	673893	0.7106	18.70
4	1034082	474832	0.1482	3.90	877649	612543	0.0000	0.00	900078	698095	0.7258	19.10
5	1088193	500853	0.1482	3.90	869518	756062	0.0000	0.00	864532	689245	0.7182	18.90
6	940273	435583	0.1482	3.90	919269	757110	0.0000	0.00	892832	646003	0.6802	17.90
7	999898	470351	0.1520	4.00	929823	880871	0.0038	0.10	877873	656301	0.6878	18.10
8	991125	459364	0.1520	4.00	895095	766474	0.0038	0.10	917882	662011	0.6878	18.10
9	997394	486445	0.1520	4.00	912584	822632	0.0000	0.00	876913	657035	0.6878	18.10
10	1010448	469927	0.1482	3.90	880680	768559	0.0000	0.00	914170	641998	0.6726	17.70
11	906426	435748	0.1520	4.00	863528	631273	0.0000	0.00	883179	668495	0.7030	18.50
12	983054	466744	0.1482	3.90	898639	764394	0.0000	0.00	858029	631413	0.6650	17.50
13	974257	436002	0.1482	3.90	898121	816342	0.0000	0.00	870384	637025	0.6650	17.50
14	1035482	453452	0.1520	4.00	883138	736309	0.0000	0.00	899975	695901	0.7220	19.00
15	1007466	487407	0.1482	3.90	865337	766454	0.0000	0.00	875237	667761	0.6992	18.40
16	1022215	496592	0.1520	4.00	888242	798699	0.0038	0.10	865277	674980	0.7106	18.70
17	920778	438140	0.1482	3.90	895060	809085	0.0000	0.00	893100	688180	0.7182	18.90
18	937946	446268	0.1520	4.00	876673	700949	0.0000	0.00	873772	680588	0.7106	18.70
19	1025292	457724	0.1482	3.90	917881	864233	0.0000	0.00	848010	675779	0.7106	18.70
20	927176	453460	0.1520	4.00	856841	719674	0.0000	0.00	910376	655510	0.6840	18.00

3.3. Analisa Hasil Pengujian

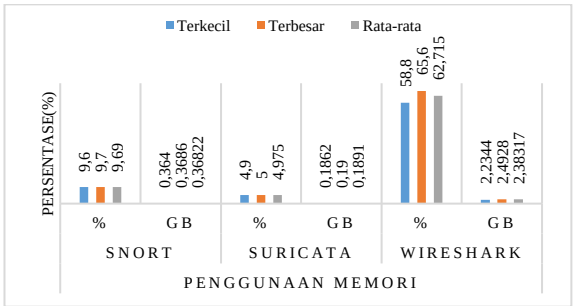
1) *Syn Flood*

Perbandingan rata-rata persentase serangan *syn flood* yang terdeteksi pada aplikasi snort, suricata dan wireshark dapat dilihat pada Gambar 3.



Gambar 3. Perbandingan Persentase Serangan *Syn Flood* Terdeteksi

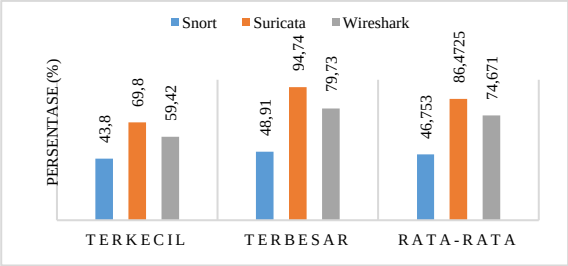
Perbandingan rata-rata penggunaan memori serangan *syn flood* yang terdeteksi pada aplikasi snort, suricata dan wireshark dapat dilihat pada Gambar 4.



Gambar 4. Perbandingan Penggunaan Memori Serangan *Syn Flood*

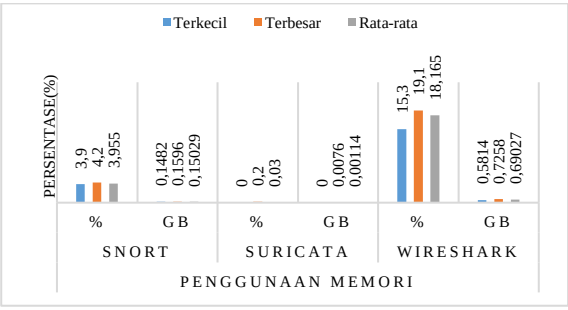
2) *Ping of death*

Hasil dari perhitungan rata-rata persentase serangan *ping of death* yang terdeteksi pada masing-masing aplikasi dapat dilihat pada Gambar 5.



Gambar 5. Perbandingan Persentase Serangan Ping of death Terdeteksi

Perbandingan rata-rata penggunaan memori serangan *ping of death* yang terdeteksi pada masing-masing aplikasi dapat dilihat pada Gambar 6.



Gambar 6. Perbandingan Penggunaan Memori Serangan *Ping of death*.

4. DISKUSI

Berdasarkan pengujian yang telah dilakukan pada jenis serangan *syn flood* dan *ping of death* disajikan rekapitulasi hasil pengujian yang dapat dilihat pada tabel 5.

Tabel 5. Rekapitulasi Hasil Pengujian

Aplikasi	Total Jumlah Serangan terdeteksi		Penggunaan Memori	
	syn flood (%)	ping of death (%)	*syn flood (GB)*	*ping of death (GB)*
snort	93.661	46.753	0.18910	0.00114
suricata	92.571	86.472	0.36822	0.15029
wireshark	94.395	74.671	2.38317	0.69027

Berdasarkan hasil pengujian menggunakan parameter total jumlah serangan yang terdeteksi bahwa wireshark memiliki rata-rata persentase serangan terdeteksi paling tinggi yaitu 94.395% dan memiliki standar deviasi 28326.74436. Urutan kedua yaitu snort 93.661% memiliki standar deviasi 24443.36969. Urutan ketiga yaitu suricata 92.571% dengan standar deviasi 45166.64817. Sementara itu pada parameter penggunaan memori, suricata memiliki rata-rata penggunaan memori paling kecil yaitu 0.1891 GB (4.975%) dibandingkan dengan snort 0.36822 GB (9.69%) dan wireshark 2.38317 GB (62.715%).

Pengujian pada jenis serangan *ping of death* dengan menggunakan parameter total jumlah serangan yang terdeteksi, suricata memiliki persentase serangan terdeteksi paling tinggi yaitu 86.472% dan memiliki standar deviasi 67736.42891. Urutan kedua adalah wireshark 74.671% yang memiliki standar deviasi 28119.24968. Urutan ketiga adalah snort 46.753% dengan standar deviasi 21226.05414. Sementara itu pada parameter penggunaan memori, suricata memiliki rata-rata penggunaan memori paling kecil yaitu 0.00114 GB (0.03%) dibandingkan dengan snort 0.15029 GB (3.955%) dan wireshark 0.69027 GB (18.165%).

Penyebab penggunaan memori yang sangat tinggi pada aplikasi wireshark karena wireshark menyimpan semua paket yang masuk saat deteksi dilakukan secara *real time* atau dalam *mode live paket capture*. Oleh karena itu, penggunaan memori wireshark menjadi sangat tinggi dibandingkan dengan snort dan suricata. Hal tersebut dikarenakan snort dan suricata memiliki kemampuan untuk mendeteksi paket yang hanya ingin dideteksi dengan cara membuat *rules*.

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan maka dapat disimpulkan suricata menjadi aplikasi yang paling efektif dalam penelitian ini dibandingkan dengan snort dan wireshark. Suricata unggul penggunaan memori di dua jenis serangan yang dilakukan dengan persentase penggunaan memori adalah 0.1891 GB (4.975%) saat serangan *syn flood* dan 0.00114 GB (0.03%) saat serangan *ping of death*. Suricata juga unggul dalam persentase total jumlah serangan *ping of death* yang terdeteksi yaitu 86.472%.

Snort menjadi aplikasi paling efektif kedua setelah suricata. Snort kalah dalam penggunaan memori di dua jenis serangan yang dilakukan dibandingkan dengan suricata, dengan persentase penggunaan memori adalah 0.36822 GB (9.69%) saat serangan *syn flood* dan 0.15029 GB (3.955%) saat serangan *ping of death*. Tetapi, snort unggul dalam penggunaan memori dibandingkan dengan wireshark yang memiliki persentase penggunaan memori 2.38317 GB (62.715%) saat serangan *syn flood* dan 0.69027 GB (18.165%) saat serangan *ping of death*.

Hasil yang didapatkan dari wireshark pada penelitian ini cukup baik, terlihat dari persentase serangan yang terdeteksi yaitu 94.395% saat serangan *syn flood* dan 74.671% saat serangan *ping of death*. Tetapi, karena penggunaan memori yang tinggi dari wireshark yaitu 2.38317 GB (62.715%) saat serangan *syn flood* dan 0.69027 GB (18.165%) saat serangan *ping of death* membuat kinerja dari komputer menjadi bekerja terlalu keras dan akibatnya adalah komputer berjalan lambat bahkan mati.

Perlu adanya penelitian lanjutan mengenai pendeteksian serangan dengan waktu serang lebih dari 1 menit agar hasilnya dapat dibandingkan dengan penelitian ini. Selain itu, penggunaan jenis serangan yang berbeda dalam melakukan pendeteksian untuk mengetahui tingkat keefektifitasan dari aplikasi snort, suricata dan wireshark.

DAFTAR PUSTAKA

[1] CNN Indonesia, "Ukraina Diserang DDoS, Diduga Serangan Siber dari Rusia," *cnnindonesia.com*, 2022. [Online]. Available: https://www.cnnindonesia.com/teknologi/20220224083642-192-763284/ukraina-diserang-ddos-diduga-serangan-siber-dari-rusia.

[2] A. M. Damar, "Kata Pengamat Soal Serangan DDoS ke Situs Pemantauan Virus Corona Pemprov Jakarta," *Liputan6.com*, 2020. [Online]. Available: https://www.liputan6.com/tekno/read/4200786/kata-pengamat-soal-serangan-ddos-ke-situs-pemantauan-virus-corona-pemprov-jakarta.

[3] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, 'Keamanan Jaringan Komputer Pada Era Big Data,' J. Sist. Informasi-J-SIKA, vol. 02, pp. 1–7, 2020.Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.

[4] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020.

[5] A. L. Ginting, J. Napitupulu, and J. Jamaluddin, "Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia," *Semin. Nas. Teknol. Inf. dan Komun.*, pp. 83–87, 2018.

[6] R. Abubakar *et al.*, "An Effective Mechanism to Mitigate Real-Time DDoS Attack," *IEEE Access*, vol. 8, pp. 126215–126227, 2020.

[7] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019.

[8] M. Fakhmi and L. M. Gultom, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis)," *Semin. Nas. Ind. dan Teknol.*, pp. 260–277, 2021.

[9] S. Sahren, "Implementasi Teknologi Firewall Sebagai Keamanan Server Dari Syn Flood Attack," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 7, no. 2, pp. 159–164, 2021.

[10] E. Acantha, M. Sampetoding, M. Natalin, E. S. Manapa, V. Yoga, and P. Ardhana, "Studi Literatur: Cara Kerja Keamanan Internet dan Kerentanan dengan TCP/IP dan DNS Literature Review: Internet Security Works and Some Basic Vulnerabilities with TCP/IP and DNS," *SainsTech Innov. J.*, vol. 3, no. 2, pp. 66–73, 2020.

[11] R. Rafli, "PENDETEKSIAN DAN PENCEGAHAN SERANGAN PADA JARINGAN MENGGUNAKAN SNORT PADA LINUX UBUNTU," *TUGAS AKHIR Jur. Manaj. Inform. Inst. AGAMA Islam NEGERI BATUSANGKAR*, vol. 66, pp. 37–39, 2018.

[12] L. F. Nainggolan, N. F. Saragih, and F. G. N. Larosa, "Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS," *Methotika J. Ilm. Tek. Inform.*, vol. 2, no. 2, pp. 1–10, 2022.

[13] H. A. S. A. L. Martanto, A. Hanif, "ANALISA SISTEM PENGEMBANGAN LOCAL AREA NETWORK (LAN) DI PT. SURYAMAS DUTAMAKMUR, Tbk," *J. AKRAB JUARA*, vol. 6, p. 6, 2021.

[14] A. Elanda and D. Tjahjadi, "Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute of Standards and Technology) Sp 800-30 (Studi Kasus Disinfolahtaau Mabes Tni Au)," *Infoman's*, vol. 12, no. 1, pp. 1–13, 2018.

[15] R. Hanipah, "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark," *J. Comput. Inf. Technol.*, vol. 4, no. 1, pp. 11–23, 2020.

[16] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8, 2018.

[17] Z. Akhyar, Hendrawaty, and Azhar, "Rancang Bangun Sistem Pengiriman Alert Instrusion Detection System Suricata Melalui Telegram," *Proceeding Semin. Nas. Politek. Negeri Lhokseumawe*, vol. 2, no. 1, pp. A175–A181, 2018.