Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202184200
Vol. 8, No. 3, Juni 2021, hlm. 517-524 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

PENGGUNAAN METODE SIGNATURED BASED DALAM PENGENALAN POLA SERANGAN DI JARINGAN KOMPUTER

Herri Setiawan [*1], M. Agus Munandar [2], Lastri Widya Astuti[3]

[1,2,3]Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Indo Global Mandiri
Email: [1]herri@uigm.ac.id *, [2]agus@uigm.ac.id, [3]lastriwidya@uigm.ac.id
*Penulis Korespondensi

(Naskah masuk: 04 Oktober 2020, diterima untuk diterbitkan: 08 Juni 2021)

Abstrak

Masalah keamanan jaringan semakin menjadi perhatian saat ini. Sudah semakin banyak *tools* maupun teknik yang dapat digunakan untuk masuk kedalam sistem secara ilegal, sehingga membuat lumpuh sistem yang ada. Hal tersebut dapat terjadi karena adanya celah dan tidak adanya sistem keamanan yang melindunginya, sehingga sistem menjadi rentan terhadap serangan. Pengenalan pola serangan di jaringan merupakan salah satu upaya agar serangan tersebut dapat dikenali, sehingga mempermudah administrator jaringan dalam menanganinya apabila terjadi serangan. Salah satu teknik yang dapat digunakan dalam keamanan jaringan karena dapat mendeteksi serangan secara *real time* adalah *Intrusion Detection System* (IDS), yang dapat membantu administrator dalam mendeteksi serangan yang datang. Penelitian ini menggunakan metode *signatured based* dan mengujinya dengan menggunakan simulasi. Paket data yang masuk akan dinilai apakah berbahaya atau tidak, selanjutnya digunakan beberapa *rule* untuk mencari nilai akurasi terbaik. Beberapa *rule* yang digunakan berdasarkan hasil *training* dan uji menghasilakan 60% hasil *training* dan 50% untuk hasil uji *rule* 1, 50% hasil *training* dan 75% hasil uji *rule* 2, 75% hasil *training* dan hasil uji rule 3, 25% hasil *training* dan hasil uji *rule* 4, 50% hasil *training* dan hasil uji untuk *rule* 5. Hasil pengujian dengan metode *signatured based* ini mampu mengenali pola data serangan melaui protokol TCP dan UDP, dan *monitoring* yang dibuat mampu mendeteksi semua serangan dengan tampilan *web base.*

Kata kunci: Keamanan, Jaringan, IDS, *Snort*, *Signatured based*

USE OF SIGNATURE BASED METHOD IN INTRODUCTION TO ATTACK PATTERNS ON COMPUTER NETWORKS

Abstract

Network security issues are becoming increasingly a concern these days. There are more and more tools and techniques that can be used to enter the system illegally, thus paralyzing the existing system. This can occur due to loopholes and the absence of a security system that protects it so that the system becomes vulnerable to attacks. The recognition of attack patterns on the network is an effort to make these attacks recognizable, making it easier for network administrators to handle them in the event of an attack. One of the techniques that can be used in network security because of a timely attack is the Intrusion Detection System (IDS), which can help administrators in surveillance that comes. This study used a signature-based method and tested it using a simulation. The incoming data packet will be assessed whether it is dangerous or not, then several rules are used to find the best accuracy value. Some rules used are based on the results of training and testing results in 60% training results and 50% for rule 1 test results, 50% training results and 75% rule 2 test results, 75% training results and rule 3 test results, 25% training results and the result of rule 4 test, 50% of training results and test results for rule 5. The test results with the signature-based method can recognize attack data patterns via TCP and UDP protocols, and monitoring is made to be able to detect all attacks with a web-based display.

Keywords: *Network, Security*, *IDS, Snort, Signatured based*

1. PENDAHULUAN

Penggunaan Internet telah banyak dimanfaatkan diberbagai bidang termasuk di dunia pendidikan, seperti halnya di Universitas Indo Global Mandiri (UIGM), salah satu perguruan tinggi di sumatera selatan. Untuk mempermudah dosen dan mahasiswa di lingkungan UIGM dalam melakukan aktifitas

proses belajar mengajar salah satunya adalah dengan memanfaatkan internet. Saat ini UIGM telah mempunyai sistem jaringan dan *server* yang digunakan dalam pengelolaan jaringan dan internet. Komputer yang terhubung ke jaringan internet, seperti *server* berpotensi sangat rentan datanya diambil oleh pihak yang tidak bertanggung jawab, kendala tersebut mengakibatkan proses dalam pertukaran data akan menjadi lambat bahkan pada kasus seperti ini bisa berakibat kerusakan sistem,. *Firewall* merupakan salah satu solusi untuk membantu menjaga keamanan jaringan komputer, tetapi jika hanya mengandalkan *firewall* saja belum menjamin keamanannya, sehingga berkembanglah teknologi yang dinamakan *Intrusion Detection System* (IDS).

Penyusup yang memasuki sistem tanpa otorisasi (*cracker*) atau penyalahgunaan previlage sumber daya sistem (*insider threat*) dapat teridentifikasi oleh IDS. IDS tidak melakukan pencegahan akan terjadinya serangan (Raharjo, 2015), namun pemanfaatan IDS dapat meminimalisir gangguan/serangan terhadap sistem yang ada dengan cara memberikan peringatan atau *alert* kepada admin jaringan.

Penelitian yang dilakukan oleh (Budiman, Iswahyudi, & Sholeh, 2014), menunjukkan jika ada serangan yang datang dari luar menuju *host* atau *server* yang terdapat IDS, maka secara otomatis akan mendeteksi dan memberitahukan kepada administrator berupa notifikasi yang dikirimkan melalui jejaring sosial Facebook, Twitter, dan Whatsapp, sehingga administrator jaringan dapat menindak lanjuti terhadap jenis serangan yang dilakukan oleh *intruder.* Pada penelitian yang lain, Mustofa *et al*. (2013) membahas tentang "Penerapan Sistem Keamanan *Honeypot* dan IDS pada Jaringan Nirkabel (*Hotspot*)", dinyatakan bahwa penerapan sistem keamanan yang berlapis dapat dilakukan dengan teknik menipu atau memberikan data palsu apabila ada penyerang yang akan masuk ke sistem atau server utama, kemudian juga honeypot akan merekam aktifitas dari penyerang dalam bentuk *log*, sedangkan snort memberikan rekaman traffik yang janggal dalam bentuk *file log* atau *alert*.

Penilaian terhadap paket data apakah berbahaya atau tidak dapat dikenali dari daftar *signatured* yang dimiliki metode *signatured based*. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data *signatured* yang ada harus tetap ter-*update* (Alamsyah, 2011).

Namun demikian, terdapat permasalahan yaitu bagaimana mengenali pola paket data serangan yang ada di jaringan dan bentuk peringatan yang akan diberikan kepada administrator, sehingga nantinya mempermudah administrator jaringan komputer dalam melakukan monitoring. Monitoring yang akan dilakukan menggunakan *tools snort* dengan menerapkan metode *signatured based* untuk mengenali pola data normal dan pola data serangan. Sehingga serangan di jaringan komputer yang dilakukan *attacker* diketahui polanya dan dapat dicegah secara otomatis.

State of the art penelitian ini adalah penggunaan metode *signatured based* dengan lima *rules* hasil dari penggabungan *rule* yang digunakan pada penelitian-penelitian terdahulu. Penggunaan *signatured based* didasari karena memiliki kelebihan dalam mendeteksi jenis serangan *port scanning*, *exploit*, dan *denial of service* sebagai usaha untuk mengantisifikasi terjadinya lagi serangan *syn flood attack* dan *sql injection* yang mengakibatkan server terkendala.

2. METODE PENELITIAN

2.1. Jaringan Komputer

Menurut Sofana (2013), jaringan komputer (*computer networks*) merupakan kumpulan interkoneksi dari berbagai komputer dan perangkat-perangkat seperti router, switch dan lain-lain, yang terhubung melalui media kabel atau media tanpa kabel (nirkabel).

2.2. Keamanan Komputer

Menurut Anilbhai & Parekh (2017) dan Pratama (2014), keamanan komputer meliputi beberapa aspek, yaitu :

a. *Confidetiality*

Confideality atau disebut juga dengan kerahasiaan merupakan tujuan utama dari keamanan komputer dan keamanan jaringan komputer. Kerahasiaan ini harus dijaga baik oleh pengguna maupun oleh sistem di dalam jaringan komputer.

b. *Integrity*

Integrity merupakan upaya untuk menjaga agar data dan informasi tidak diubah oleh pihak yang tidak berhak, sehingga keabsahan data dan informasi tetap terjaga.

c. *Availability*

Availability atau ketersediaan merupakan upaya untuk menyediakan akses dan otoritas kepada pihak-pihak yang berhak terhadap data dan informasi tersebut, dengan adanya *availability* ini maka secara jelas ditampilkan siapa saja yang memiliki hak terhadap akses sistem.

2.3. Intrusion Detection System (IDS)

Menurut Jabez & Muthukumar (2015) dan Azeez, Bada, Misra, & Adewumi (2020), *Intrusion Detection System* (IDS) adalah perangkat lunak yang memantau sistem jaringan terhadap pelanggaran atau aktivitas berbahaya atas kebijakan, kemudian membuat laporan ke manajemen sistem. Fokus utama dari IDS yaitu mengidentifikasi kemungkinan insiden yang akan terjadi dan mencatat informasinya. IDS tidak melakukan pencegahan terjadinya serangan (Hanafi, Raharjo, & Suraya, 2015), namun pemanfaatan IDS dapat meminimalisir gangguan/serangan terhadap sistem yang ada dengan cara memberikan peringatan atau *alert* kepada admin jaringan.

2.4. Jenis Intrusion Detection System (IDS)

Pendeteksian dalam implementasi IDS ada beberapa jenis yaitu (Stiawan, Abdullah, & Idris, 2010):

a. *Signature based detection*

Pendektesian jenis ini dapat dikonfigurasi dengan dengan mudah dan cepat. Walaupun dalam hal deteksi serangan jenis ini terbatas, tapi memiliki tingkat keakuratan yang lebih.
Signature based memiliki kelebihan dalam mendeteksi jenis serangan *port scanning*, *exploit*, dan *denial of service* (Sugeng & Theta, 2015).

b. *Anomaly based detection*

Metode ini berguna untuk mendeteksi paket-paket yang tidak diinginkan, berupa paket yang tidak valid karena tidak normal.

c. *Stateful protocol inspection*

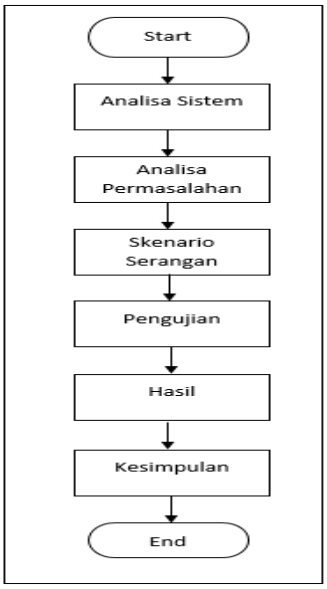
Basis pendektisian adalah adanya *anomaly*, namun dapat menganalisa lapisan *network* dan lapisan *protocol* dalam OSI.

2.5. Snort

Snort adalah sebuah perangkat lunak yang berfungsi untuk memberikan laporan ke administrator jika terdapat aktifitas-aktifitas mencurigakan pada data yang masuk. *Snort* pertama kali dibuat dan dikembangkan oleh Martin Roesch, lalu menjadi *open source project* (www.snort.org).

2.6. Alur Penelitian

Langkah kerja penelitian yang dilakukan mulai dari persiapan awal hingga kesimpulan akhir ini terbagi atas beberapa tahapan seperti terlihat pada Gambar 1, hal ini dilakukan agar dalam penelitian ini dapat lebih terarah dan terstruktur sehingga mencapai target sesuai waktu yang ditentukan.

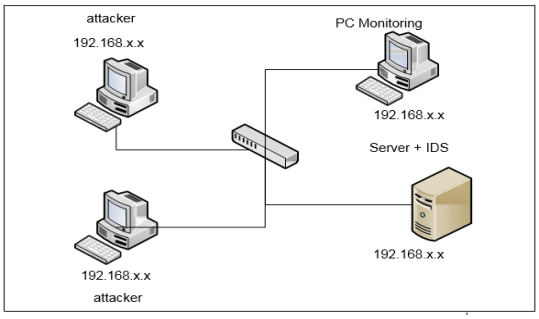


Gambar 1. Diagram Alir Penelitian

2.7. Analisa Permasalahan

Penelitian dilakukan di Universitas Indo Global Mandiri (UIGM) yaitu dengan menganalisa masalah keamanan pada *web server*. W*eb server* yang terdapat di UIGM masih rentan terhadap serangan-serangan yang dilakukan oleh penyusup, dikarenakan pernah terjadi serangan *syn flood attack* dan *sql injection* yang mengakibatkan server terkendala dan terdapat beberapa data yang berhasil dikses secara ilegal. Diperlukan suatu cara untuk menjaga keamanan *server* sehingga mampu meminimalisir serangan-serangan terhadap *server* yang ada di jaringan terutama *web server*. Aplikasi pendeteksian yang diperlukan adalah aplikasi yang dapat mendeteksi adanya serangan pada sistem jaringan yaitu aplikasi *intrusion detection system* (IDS).

2.8. Skenario Serangan



Gambar 2. *Skenario Syn Flooding*

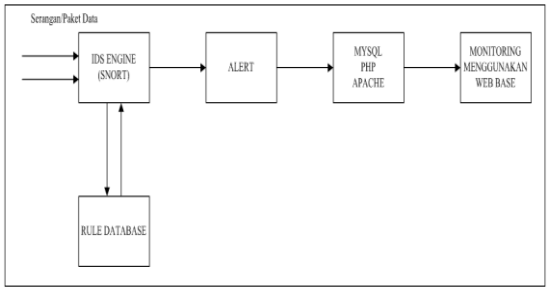
Perangkat keras (*hardware*) yang digunakan adalah sebagai berikut :

1. Satu unit komputer sebagai *Web Server* dan IDS
2. Dua unit Komputer sebagai *attacker.*
3. Satu unit Komputer/laptop sebagai *monitoring*.

Cara kerja skenario serangan seperti terlihat pada gambar 2 adalah salah 1 (satu) pc penyerang akan menyerang ke *server* IDS baik itu menyerang protokol TCP, HTTP maupun UDP, dimana saat terjadinya serangan admin akan memantau pada pc monitoring apabila terjadi serangan, ataupun cara kerja serangan dengan 2 (dua) penyerang yang langsung menyerang ke *server*, dan admin dapat memantau melalui pc monitoring yang ada, sehingga apabila terjadi nya serangan IDS akan memberikan *alert* yang dapat dilihat admin melalui pc monitoring yang sudah berbentuk *webbase*. Serangan yg diujikan terhadap target selama penelitian menggunakan aplikasi LOIC dan Hping3. PC 1 sebagai attacker dan PC 2 sebagai target (server)

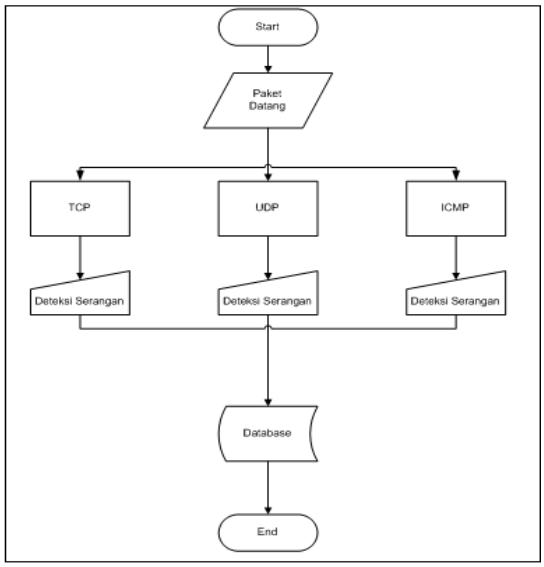
2.9. Skema Kerja IDS

Knowledge based/Signatured Based IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* IDS, yang berisi *signatured-signatured* paket serangan (Gambar 3). Apabila paket data mempunyai pola yang sama dengan salah satu pola yang ada di *database rule* IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola yang terdapat di *database rule* IDS, maka paket data tersebut dianggap bukan merupakan serangan, kemudian IDS *engine* akan membaca *alert* dari IDS.



Gambar 3. Skema Kerja IDS

Pada gambar 4 menunjukkan diagram alir dari proses pembuatan *rule snort*, dimana pada saat ada paket datang, baik itu dalam bentuk protokol *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP), maupun *Internet Control Message Protocol* (ICMP), apabila protokol yang masuk tersebut dianggap mencurigakan maka selanjutnya akan dibuat *rules* yang kemudian dimasukkan kedalam *database snort*.



Gambar 4. *Flowchart* Proses *Rule Snort*

3. PEMBAHASAN DAN HASIL

Berdasarkan gambar 2, skenario serangan yang diujikan adalah salah 1 (satu) atau 2 (dua) pc penyerang akan menyerang ke *server* IDS melalui protokol TCP, HTTP maupun UDP. Saat terjadinya serangan admin akan memantau pada pc monitoring, sehingga IDS akan memberikan *alert* yang dapat dilihat admin melalui pc monitoring yang sudah berbentuk *webbase*.

3.1. Pengujian

Pengujian dilakukan dengan menggunakan 5 (lima) buah *rules*, adapun *rule* yang digunakan adalah sebagai berikut :

1. Rule 1 (satu)

```
Alert tcp $EXTERNAL_NET any ->
$HOME_NET $HTTP_PORTS
(msg:"Slowloris DoS tool flood";
detection_filter:track by_src, count 20,
seconds 20; metadata:service http;
classtype:attempted-dos; sid:1234572; rev:2;)
```

Sumber : https://github.com/John-Lin/docker-snort/blob/master/snortrules-snapshot-2972/rules/server-other.rules

Rule ini akan mengenali pola serangan dimana pada *rule* ini akan memberikan keterangan bahwa *snort* akan memberikan peringatan pada paket data dengan protokol berjenis TCP, *rule* ini akan memberikan pesan Slowloris DoS tool flood dengan nomor id 1234572 versi 2 (dua), pada *rule* ini akan mencatat apabila selama 20 detik terdapat minimal 20 peristiwa berdasarkan IP sumber yang sama, setelah melakukan pencatatan waktu akan diulang kembali dari 0.

2. Rule 2 (dua)

```
Alert tcp any any -> any any (msg:"Possible SYN flood"; classtype:attempted-dos; sid:1999999; flags:S;  flow: stateless; detection_filter: track by_dst, count 50, seconds 10;)
```

Sumber : https://dubell.io/creating-syn-flood-attacks-with-python/

Rule ini akan mengenali pola serangan dimana pada *rule* ini akan memberikan keterangan bahwa *snort* akan memberikan peringatan pada paket data dengan protokol berjenis tcp, *rule* ini akan memberikan pesan Possible SYN flood dengan nomor id 1999999, *rule* ini akan mencatat apabila selama 10 detik terdapat minimal 50 peristiwa berdasarkan IP sumber yang sama dan *rule* ini akan mendeteksi jika ada *flags* yang berjenis Syn.

3. Rule 3 (tiga)

```
Alert tcp any any ->any any (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20,seconds 60; sid:5000001;rev:1;)
```

https://www.researchgate.net/publication/262345832_Using_network_packet_generators_and_snort_rules_for_teaching_denial_of_service_attacks

Rule ini akan mengenali pola serangan dimana pada *rule* ini akan memberikan keterangan bahwa *snort* akan memberikan peringatan pada paket data dengan protokol berjenis tcp, *rule* ini akan memberikan pesan TCP SYN flood attack detected dengan nomor id 5000001 dan menggunakan versi 1 (satu), *rule* ini akan mencatat apabila selama 60 detik terdapat minimal 20 peristiwa berdasarkan IP sumber yang sama.*Flags* adalah kontrol bit yang menandakan atau menunjukkan *connection states* yang berbeda atau informasi begaimana sebuah paket harus ditangani. Pada *rule* 3 ini*snort* akan memberikan *alert* apabila terdapat paket dengan *flags* S (SYN). *Threshold* digunakan untuk mengurangi jumlah *event* yang dicatat dari sebuah *rule*, perintah *threshold* membatasi jumlah peristiwa yang dicatat selama interval waktu tertentu

4. Rule 4 (empat)

```
Alert udp any any -> any 80 (msg:"SLR - LOIC DoS Tool UDP Mode)"; content:"|65 73 75 64 65 73 75 64 65 73 75 7e|"; threshold: type threshold, track by_src, count 100 , seconds 5; sid:1234571; rev:1; )
```

Sumber : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/loic-ddos-analysis-and-detection/

Rule ini akan mengenali pola serangan dimana pada *rule* ini akan memberikan keterangan bahwa *snort* akan memberikan peringatan pada paket data dengan protokol berjenis udp, rule ini akan memberikan pesan SLR – LOIC DoS Tool UDP Mode dengan nomor id 1234571 dengan menggunakan versi 1, *rule* ini akan mencatat apabila selama 5 detik terdapat minimal 100 peristiwa berdasarkan IP sumber yang sama dan akan mengenali berdasarkan *content* dan juga *threshold.*

5. Rule 5 (lima)

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SLR – LOIC DoS Tool – Behavior Rule (tracking/threshold)"; threshold: type threshold, track by_src, count 100, seconds 5; reference: url,; classtype:misc-activity; sid:1234590; rev:1;)
```

Sumber : www.simpleweb.org/reports/loic-report.pdf

Rule ini akan mengenali pola serangan dimana pada *rule* ini akan memberikan keterangan bahwa *snort* akan memberikan peringatan pada paket data dengan protokol berjenis tcp, *rule* ini akan memberikan pesan SLR – LOIC DoS Tool – Behavior Rule, *rule* ini akan mencatat apabila selama 5 detik terdapat minimal 100 peristiwa berdasarkan IP sumber yang sama.

3.2. Hasil

Pengujian dilakukan untuk mengetahui tingkat ketepatan pada pengenalan pola serangan, pada pengujian ini dilakukan dengan menggunakan *5 rules*. Mungukur tingkat akurasi yang didapatkan dengan menggunakan rumus:

$$\text{accuracy} = \frac{\textit{Jumlah data pengujian yang benar}}{\textit{Jumlah data yang di uji}} \text{ x } 100\% \quad (1)$$

Hasil pengujian dapat dilihat pada Tabel 1.

Tabel 1. *Perbandingan Hasil Uji Rule*

No.	Serangan	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5
1.	LOIC (HTTP)	T	T	T	TT	T
2.	LOIC (TCP)	T	TT	T	TT	T
3.	LOIC (UDP)	T	TT	TT	T	TT
4.	HPING3	T	TT	T	TT	TT
5.	LOIC (HTTP)	T	T	T	TT	T
6.	LOIC (TCP)	T	TT	T	TT	T
7.	LOIC (UDP)	TT	TT	TT	T	TT
8.	HPING3	TT	TT	T	TT	TT

No.	Serangan	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5
9.	LOIC (HTTP)	T	T	T	TT	T
10.	LOIC (TCP)	T	T	T	TT	T
11.	LOIC (UDP)	TT	TT	TT	T	TT
12.	HPING3	TT	TT	T	TT	TT
13.	LOIC (HTTP)	T	T	T	TT	T
14.	LOIC (TCP)	T	T	T	TT	T
15.	LOIC (UDP)	TT	TT	TT	T	TT
16.	HPING3	TT	T	T	TT	TT
17.	LOIC (HTTP)	T	T	T	TT	T
18.	LOIC (TCP)	T	T	T	TT	T
19.	LOIC (UDP)	TT	TT	TT	T	TT
20.	HPING3	TT	T	T	TT	TT

Keterangan :
T = Terdeteksi
TT = Tidak Terdeteksi

Hasil menggunakan *rule* 1, nilai akurasi yang didapatkan adalah:

$$Accuracy = \frac{12}{20} x\ 100\ \% = 60\ \%$$

Hasil menggunakan rule 2, nilai akurasi yang didapatkan adalah:

$$Accuracy = \frac{10}{20} x\ 100\ \% = 50\ \%$$

Hasil menggunakan rule 3, nilai akurasi yang didapatkan adalah:

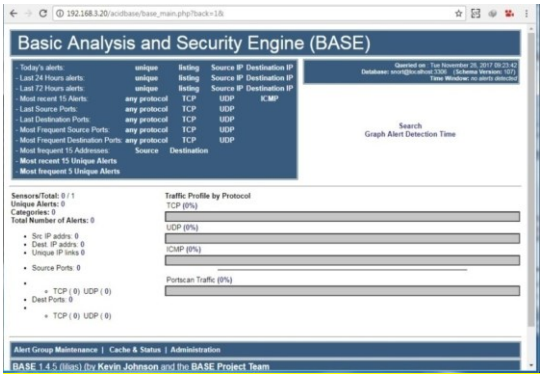
$$Accuracy = \frac{15}{20} x\ 100\ \% = 75\ \%$$

Hasil menggunakan rule 4, nilai akurasi yang didapatkan adalah:

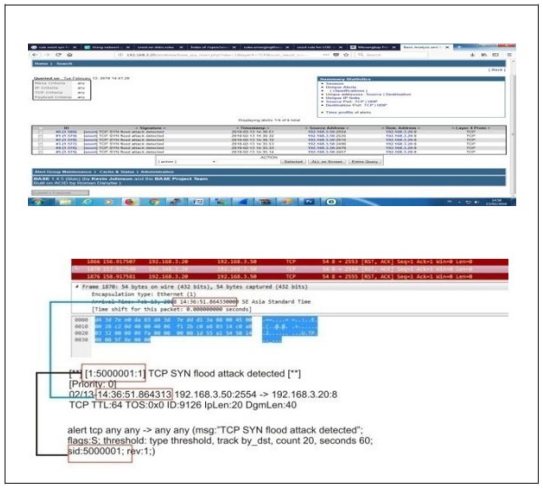
$$Accuracy = \frac{5}{20} x\ 100\ \% = 25\ \%$$

Hasil menggunakan rule 5, nilai akurasi yang didapatkan adalah:

$$Accuracy = \frac{10}{20} x\ 100\ \% = 50\ \%$$



Gambar 5. Sebelum menggunakan snort



Gambar 6. *Hasil deteksi*

Gambar 5 menunjukkan sebelum menggunakan snort, hasil monitoring nya tidak ada alarm peringatan, sedangkan gambar 6 menunjukkan *alert* yang dihasilkan oleh *snort,* hasil yang ditampilkan snort dibandingkan dengan hasil yang diambil menggunakan *tcpdump* untuk melihat waktu yang dihasilkan apakah sama dengan waktu yang diberikan oleh IDS. Berdasarkan hasil yang didapat, kinerja dari integritas antara sistem operasi dan *snort* sangat baik, dengan kecepatan deteksi *threat* yang cukup akurat, terlihat pada saat dilakukan pengujian, IDS memberikan sebuah *alert message* secara bersamaan dengan pendeteksian. Snort IDS memilki *rules* yang dapat digunakan secara bebas, *rule* tersebut dapat dibuat sesuai dengan kebutuhan dengan mengedit *files local rules*. Untuk penerapan *rule* yang akan digunakan di UIGM digunakan kombinasi dari beberapa *rule* yang telah diujikan di atas, yaitu penggunaan *rule* 3 dan *rule* 4 direkomendasikan untuk diterapkan di UIGM.

Hasil pengujian yang telah dilakukan dinilai baik dan akurat dilihat dari waktu serangan dengan data waktu yang ditunjukkan pada monitoring yang dihasilkan, *snort* dan *rule* yang diterapkan mampu menangkap tindakan penyusupan dengan tepat, dan juga dari false positif yang dihasilkan. Hasil pengujian pada *rule* 3 dapat mendeteksi serangan dengan tingkat akurasi 75%, dengan pengenalan waktu keamanan dapat mencapai 24 jam selama *server* aktif.

Berdasarkan perbandingan sebelum dan sesudah menggunakan snort, dapat terlihat dengan jelas peran *signatured based* IDS dalam mendeteksi serangan dengan mengirimkan alarm peringatan bahwa telah terjadinya serangan kedalam server.

4. KESIMPULAN

1. Pengujian yang dilakukan dengan menggunakan 5 *rule* mampu mendeteksi

semua serangan DDoS, dengan hasil *rule* 1 mampu mendeteksi 60% untuk hasil *training* dan 50% untuk hasil uji, *rule* 2 mampu mendeteksi 50% untuk hasil *training* dan 75% untuk hasil uji, *rule* 3 mampu mendeteksi 75% untuk *training* dan hasil uji, *rule* 4 mampu mendeteksi 25% untuk hasil *training* dan hasil uji, dan *rule* 5 mampu mendeteksi 50% untuk hasil *training* dan hasil uji.

2. Metode *signatured based* yang diterapkan mampu mengenali pola data serangan dalam mendeteksi protokol TCP dan UDP.
3. *Monitoring* yang dibuat mampu mendeteksi semua serangan dengan tampilan *web base*.

DAFTAR PUSTAKA

ALAMSYAH. 2011. Implementasi keamanan instrusion detection system (ids) dan instrusion prevention system (ips) menggunakan clearos. *SMARTek, 9*(3), 223–229.

ANILBHAI, S. P., & PAREKH, C. (2017). Intrusion Detection and Prevention System for IoT. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *2*(6), 771–776.

AZEEZ, N. A., BADA, T. M., MISRA, S., & ADEWUMI, A. (2020). Intrusion Detection and Prevention Systems : An Updated Review Intrusion Detection and Prevention Systems : An Updated Review, (October 2019). https://doi.org/10.1007/978-981-32-9949-8

BUDIMAN, S. A., ISWAHYUDI, C., & SHOLEH, M. 2014. Implementasi Intrusion Detection System (IDS) Menggunakan Jejaring Sosial Sebagai Media Notifikasi. In *Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014*. Yogyakarta.

HANAFI, M. I. H., RAHARJO, S., & SURAYA. (2015). Implementasi Konsep Multi-Nas Dengan Mengintegrasikan VPN Server dan Freeradius Server dalam Membangun Sistem Otentikasi Jaringan Wifi. *JARKOM*, *3*(1), 16–27.

JABEZ, J., & MUTHUKUMAR, B. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. In *Procedia - Procedia Computer Science* (Vol. 48, pp. 338–346). Elsevier Masson SAS. https://doi.org/10.1016/j.procs.2015.04.191

MUSTOFA, M. M., & ARIBOWO, E. (2013). Penerapan Sistem Keamanan Honeypot dan Ids Pada Jaringan Nirkabel (Hotspot). *Sarjana Teknik Informatika*, *1*(1), 111–118.

PRATAMA, I. P. A. E. (2014). *Handbook Jaringan Komputer : Teori dan Praktek Berbasiskan Open Source*.

PROJECT, T. S. (2020). *Users Manual 2.9.16*. Cisco and/or its affiliate. Retrieved from https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20200919%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200919T201228Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=433c3625794f2ce37c6c8b4acfa7fe3450db0404f3d25c324e740e4e9d648b72

SOFANA, I .2013. *Membangun Jaringan Komputer : Mudah Membuat Jaringan Komputer (Wire & Wireless) Untuk Pengguna Window Dan Linuk*. Bandung: Informatika.

STIAWAN, D., ABDULLAH, A. H., & IDRIS, M. Y. (2010). Classification of Habitual Activities in Behavior-based Network Detection, *2*(8), 1–7.

SUGENG, W., & THETA. (2015). *Jaringan Komputer Dengan TCP/IP (Edisi Revisi)*. Surakarta: Informatika.

Halaman ini sengaja dikosongkan