JOISIE Journal Of Information System And Informatics Engineering
Vol. 7, No.2, Desember 2023, Hlm 381-389

p- ISSN: 2503-5304
e- ISSN: 2527-3116

IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN RULE-BASED IDS PADA PT NETKRIDA TUAH CAKRAWALA

Debi Setiawan[1)], M.Charlie Pratama[2)], Diki Arisandi [3)]
[1-3] Teknik Informatika, Universitas Abdurrab
email: [1]debisetiawan@univrab.ac.id, [2]charliepratama@student.univrab.ac.id, [3]dikiarisandi@univrab.ac.id

Abstract

Network security systems are critical to protect data and information systems from cyber attacks. PT Netkrida Tuah Cakrawala is a company engaged in information technology that has an extensive computer network. However, this company does not have an adequate network security system, thus increasing the risk of cyber attacks. This research aims to implement a network security system using Rule-Based IDS at PT Netkrida Tuah Cakrawala. This research was conducted using the NDLC (network development life cycle) method. The results showed that the implementation of Rule-Based IDS at PT Netkrida Tuah Cakrawala can improve the company's network security. This system can detect and report suspicious activities on the network, such as port scanning attacks, DoS attacks, and SQL injection attacks. Based on the results of this research, it can be concluded that the implementation of Rule-Based IDS is the right step to improve the company's network security. This system can prevent cyber attacks and protect company data and information systems.

Keywords: *Netkrida Tuah Cakrawala, IDS, NDLC, Rule-based, Network security.*

Abstrak

Sistem keamanan jaringan merupakan hal yang penting untuk melindungi data dan sistem informasi dari serangan cyber. PT Netkrida Tuah Cakrawala adalah perusahaan yang bergerak di bidang teknologi informasi yang memiliki jaringan komputer yang luas. Namun, perusahaan ini belum memiliki sistem keamanan jaringan yang memadai, sehingga meningkatkan risiko terjadinya serangan cyber. Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan jaringan menggunakan Rule-Based IDS pada PT Netkrida Tuah Cakrawala. Penelitian ini dilakukan dengan menggunakan metode NDLC (network depelovment life cycle). Hasil penelitian menunjukkan bahwa implementasi Rule-Based IDS pada PT Netkrida Tuah Cakrawala dapat meningkatkan keamanan jaringan perusahaan. Sistem ini dapat mendeteksi dan melaporkan aktivitas yang mencurigakan di jaringan, seperti serangan port scanning, serangan DoS, dan serangan SQL injection. Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa implementasi Rule-Based IDS merupakan langkah yang tepat untuk meningkatkan keamanan jaringan perusahaan. Sistem ini dapat mencegah terjadinya serangan cyber dan melindungi data dan sistem informasi perusahaan.

Kata Kunci : *Netkrida Tuah Cakrawala, IDS, NDLC, basis aturan, keamanan jaringan*

1. PENDAHULUAN

Pada era global saat ini, perkembangan teknologi terus menerus meningkat pesat namun dibalik perkembangan terknologi yang pesat pula tingkat ancaman kejahatan di dunia maya (cybercrime) pun ikut meningkat juga(Habibi & Liviani, 2020), teknologi yang pada dasarnya dikembangkan untuk mempermudah segala kegiatan manusia bisa saja berbalik menjadi ancaman tak terduga bagi pengguna teknologi tersebut(Nafi'ah, 2020).

Dikutip pada halaman kominfo.go.id, Indonesia menjadi negara no 2 sebagai korban cybercrime didunia(Danuri & Suharnawi, 2017), berbagai kejahatan yang telah terjadi sebagai seorang pengelola server jaringan dan internet (system administrator) harus memiliki rasa tanggung jawab terhadap keamanan system tersebut(Napitupulu, 2017).

Cybercrime merupakan kejahatan yang dilakukan melalui jaringan internet atau komputer(Suhaemin & Muslih, 2023). Di Indonesia, terdapat beberapa jenis cybercrime yang sering terjadi dan marak terjadi di Indonesia seperti penipuan online melalui situs jual beli online atau penipuan melalui email

palsu(Erdiyanto, 2023)(Hasanah et al., 2023), Pencurian data pribadi maupun data perusahaan, Serangan malware seperti virus, worm, atau trojan horse juga sering terjadi di Indonesia(Surahman, 2023)(Faizal et al., 2023), Defacing situs web dengan tujuan merusak atau mengubah informasi yang ada di dalamnya(Faizal et al., 2023), Cyberbullying berupa tindakan intimidasi atau pelecehan yang dilakukan melalui media sosial atau internet(Amin et al., 2023) .

Meskipun Indonesia telah memiliki beberapa undang-undang yang mengatur kejahatan cyber, seperti UU ITE dan UU PDP, namun masih banyak kelemahan dalam sistem keamanan siber di Indonesia. Beberapa faktor yang menyebabkan kelemahan tersebut antara lain kurangnya kesadaran masyarakat tentang keamanan siber, kurangnya sumber daya manusia yang ahli di bidang keamanan siber, dan kurangnya dukungan teknologi yang memadai(Ariyaningsih et al., 2023)(Ariyaningsih et al., 2023).

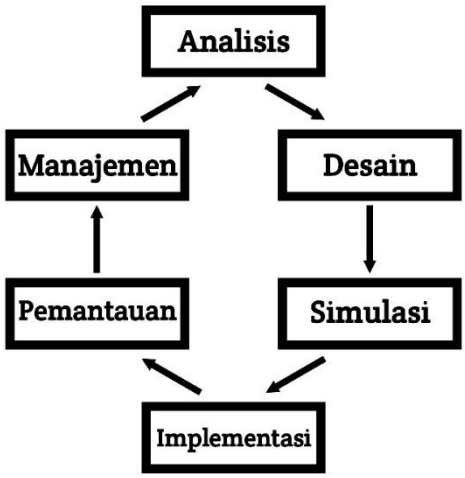
Oleh karena itu, sangat diperlukan sebuah cara untuk mengantisipasi tindakan-tindakan cybercrime yang mengintai pengguna jaringan atau internet, Intrusion Detection System (IDS) adalah sebuah system yang mampu mendeteksi aktivitas mencurigakan dalam sebuah system atau jaringan dengan menggunakan perangkat lunak (software) yang bernama Snort (Alfaeni & Fahriani, n.d.).

Bagi sebuah perusahaan sangat dibutuhkan tingkat keamanan jaringan yang memadai untuk selalu terjaga dari tindakan kejahatan terkhususnya pencurian data(Jufri & Heryanto, 2021). karena akan berefek besar dan sangat merugikan bagi pihak perusahaan, maka dari itu menggunakan metode IDS sebagai sarana untuk melindungi hal-hal yang bersifat rahasia merupakan salah satu langkah yang baik untuk memastikan tidak ada kebocoran data yang terjadi(Alfaeni & Fahriani, n.d.)(Alfaeni & Fahriani, n.d.), melalui penelitian ini diharapkan akan meminimalisir tindakan kejahatan yang akan terjadi. Tujuan dari penelitian ini adalah Menciptakan sebuah jaringan internet yang punya sistem pertahanan dan keamanan yang terjamin bagi PT.Netkrida Tuah Cakrawala dan terhindar dari pelaku kejahatan atau cybercrime, dan membuktikan Metode IDS menggunakan snort terbukti sebagai system mampu memonitoring aktivitas-aktivitas user di internet demi mencegah pencurian data maupun tindakan kejahatan lainnya(Alfaeni & Fahriani, n.d.) (Ilham et al., 2023).

Intrusion Detection System (IDS) adalah sebuah sistem keamanan komputer yang dirancang untuk mendeteksi aktivitas tidak sah atau mencurigakan pada sebuah perangkat atau jaringan komputer(Purnama et al., 2023). IDS memantau lalu lintas jaringan untuk intrusi dan aktivitas mencurigakan dan melaporkannya dalam bentuk peringatan atau alarm(Puntadheva et al., 2022). IDS dapat berupa aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan pada jaringan komputer, Tujuan dari IDS adalah untuk mengidentifikasi akses tidak sah yang masuk ke dalam sistem dan memberikan peringatan kepada pengguna agar dapat mengambil tindakan yang tepat, IDS dapat membantu mencegah akses ilegal masuk ke dalam sistem dan menjaga keamanan server, Namun perlu diingat bahwa IDS hanya berperan untuk memberi peringatan dan tidak bisa memblokir (filter) serangan yang terjadi, IDS dapat diatur dan dikonfigurasi sesuai dengan kebutuhan dan tujuan penggunaan.

2. METODE PENELITIAN

Kerangka penelitian adalah konsep pada penelitian yang saling berhubungan, dimana penggambaran variabel satu dengan lainnya bisa terkoneksi secara detail dan sistematis, Kerangka penelitian dibuat agar penelitian bisa lebih mudah dipahami karena nantinya dalam laporan penelitian penyampaiannya bisa runtut, Kerangka penelitian juga membantu peneliti untuk memaparkan konsep-konsep penelitian secara sistematis dan dapat diterima oleh semua pihak, Kerangka penelitian terdiri dari beberapa unsur, seperti kerangka konsep, kerangka teori, kerangka metodologi, dan kerangka analisis data, berikut adalah bentuk dari kerangka penelitian.



Gambar 1. Framework NDLC

kerangka penelitian yang akan diimplementasikan kerangka penelitian NDLC (Network Development Life Cycle) pada PT.Netkrida Tuah Cakrawala

Tabel 1. Langkah-langkah Kinerja Penelitian

Tahapan	**Kegiatan**	**Hasil/Tools**
	Mulai	
Tahap Analisis	Identifikasi Masalah Perumusan Masalah	Hasil Analisis Gambaran MasalahStudi Kepustakaan
Tahap Desain	Mengumpulkan Informasi yang dibutuhkan	- Wawancara - Observasi
Tahap Simulasi	Analisa dan Perancangan IDS Simulasi	- Snort - NIDS - Rule-based IDS - VirtualBox - NPCAP - LIBPCAP
Tahap Implementasi	Pengembangan IDS Implementasi	- Snort - NIDS - Rule-based IDS - NPCAP - LIBPCAP
Tahap Pemantauan	Pengujian kinerja IDS dengan melakukan monitoring	- Reporting
Tahap Manajemen	Mengevaluasi cara kerja dan hasil kerja dari metode IDS yang telah diterapkan	
	Selesai	

2.1 ANALISIS (ANALYSIS)

Tahap ini melibatkan analisis kebutuhan sistem jaringan komputer dan identifikasi masalah keamanan yang perlu diatasi oleh IDS pada PT.Netkrida Tuah Cakrawala, melakukan analisis tentang kebutuhan sistem jaringan komputer dan identifikasi masalah keamanan yang perlu diatasi oleh IDS dan tahapan ini akan dimulai dengan berdiskusi kepada pihak PT.Netkrida Tuah Cakrawala tentang permasalah yang terjadi pada PT Mereka hingga menganalisa akar dari permasalahan yang terjadi,

Hasil analisi meliputi beberapa hal sebagai berikut :

1. Jenis perangkat yang tersedia pada PT Netkrida Tuah Cakrawala adalah 1 Modem dan 5 PC aktif yang digunakan oleh seluruh komposisi perusahaan PT Netkrida Tuah Cakrawala.
2. Sistem operasi yang digunakan pada PT Netkrida Tuah Cakrawala meliputi 3 PC dengan sistem operasi windows dan 2 PC dengan system operasi linux, Para user menggunakan lebih banyak PC dengan sistem operasi windows untuk keperluan sehari-hari, dan beberapa PC dengan sistem operasi linux untuk beberapa kebutuhan perusahaan.
3. Internet Service Provider (ISP) yang digunakan oleh PT Netkrida Tuah Cakrawala adalah ISP dari Telkomsel yang kita kenal dengan Indihome, PT Netkrida Tuah Cakrawala berlangganan internet broadband dari Indihome dengan bandwidth 30 Mbps.
4. Masalah yang dialami oleh PT Netkrida Tuah Cakrawala antara lain adalah sering terjadinya gangguan pada jaringan seperti loading untuk akses internet yang terasa lambat, sehingga menimbulkan beberapa kerugian seperti reputasi perusahaan karena dinilai lambat merespon dan produktifitas perusahaan karena ketersediaan jaringan internet yang dinilai sangat lambat

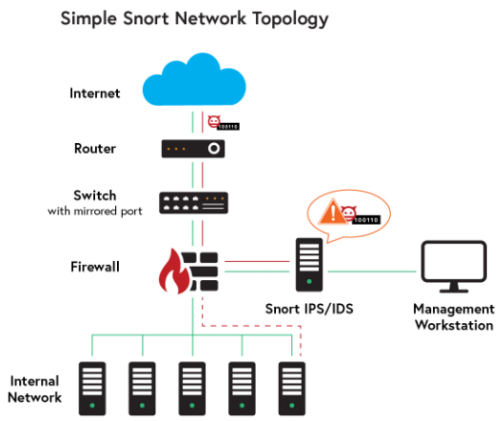
Perusahaan sudah mencoba beberapa cara antara lain menginstall ulang sistem operasi tiap PC, meningkatkan bandwidth, dan mencoba beberapa antivirus tapi tetap tidak membuahkan hasil, maka dari itu PT Netkrida Tuah Cakrawala tertarik untuk mencoba metode Intrusion Detection System (IDS) oleh Snort yang ditawarkan oleh peneliti. Bagi peneliti ada kemungkinan terjadinya TCP/UDP Attack atau Port Scanning

2.2 DESAIN (DESIGN)

Tahap ini membutuhkan penelitian lebih lanjut dan detail tentang perancangan infrastruktur jaringan yang aman dan terstruktur untuk mendukung implementasi IDS. Hal ini meliputi pemilihan perangkat keras dan perangkat lunak yang sesuai, serta perencanaan topologi jaringan pada PT.Netkrida Tuah Cakrawala.

2.3 SIMULASI PROTOTYPE

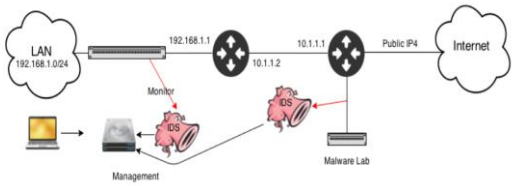
Tahap ini peneliti akan memnentukan tools yang akan digunakan beserta metode-metode di dirasa cocok untuk menjadi sebuah solusi pagi PT Nerkrida Tuah Cakrawala, tentu peneliti ini akan mulai dengan menentukan topologi umum yang biasanya digunakan untuk implementasi IDS, kemudian dilanjutkan metode-metode yang akan digunakan, berikut contoh topologi umum yang biasa digunakan untuk IDS



Gambar 2. Topologi Umum Snort

Topologi diatas menjelaskan bahwa snort memiliki fungsi sebagai pertahanan ganda setelah firewall, hal ini yang menyebabkan sebuah system yang memiliki snort akan sangat rumit untuk dijadikan korban intrusi(Suhaemin & Muslih, 2023). Dengan fungsi-fungsi tersebut, IDS menjadi salah satu komponen penting dalam mengamankan jaringan komputer dari serangan dan aktivitas yang mencurigakan,

Setelah itu maka akan ditentukannya Metode yang akan digunakan pada Snort, Rule-Based yang merupakan sebuah metode yang dapat membuat sebuah sistem keamanan jaringan yang lebih fleksibel tentu menjadi opsi utama bagi peneliti untuk mengatasi permasalahan pada PT Netkrida Tuah Cakrawala, Berikut contoh penerapan Snort menggunakan metode Rule-Based



Gambar 3. Rule Based Snort

IDS berbasis aturan ini memeriksa lalu lintas jaringan dan membandingkannya dengan seperangkat aturan yang telah ditentukan sebelumnya. Jika lalu lintas jaringan cocok dengan aturan, IDS akan mengklasifikasikannya sebagai serangan dan mengambil tindakan yang sesuai, berikut beberapa parameter yang digunakan oleh IDS(Haryani & Raharjo, 2021):

1. Header : Bagian dari paket jaringan yang digunakan untuk mengidentifikasi sumber dan tujuan. Seperti IP Addresses dan Direction Operator.
2. Payload : Data yang dikirimkan melalui jaringan. Payload dapat berisi data seperti teks, gambar, video, atau file lainnya.
3. Protocol : Protokol jaringan yang digunakan untuk mengirimkan data. Seperti HTTP, FTP, SMTP, Telnet dll
4. Port : Nomor port yang digunakan untuk mengirimkan data.
5. Setelah menentukan topologi dan metode yang akan digunakan maka peneliti akan melanjutkan penelitian ke tahap simulasi, peneliti menggunakan vitrualbox sebagai sebuah aplikasi yang dapat menggambar kinerja IDS Snort melalui ruang virtual.

2.4 IMPLEMENTASI

Tahap ini melibatkan implementasi IDS pada sistem jaringan komputer, Implementasikan IDS pada sistem jaringan komputer yang telah dirancang. Pastikan bahwa IDS dapat memantau dan mendeteksi serangan yang terjadi, pada tahapan ini tentu peneliti tidak lagi menggunakan virtualbox untuk melakukan simulasi kinerja dari Snort, melainkan peneliti akan mengimplementasikan IDS pada perangkat nyata dari PT Netkrida Tuah Cakrawala dengan menyesuaikan konfigurasi yang sebelumnya digunakan pada virtualbox maka kita siap masuk ke tahap selanjutnya.

2.5 MONITORING

Tahap ini melibatkan pemantauan sistem jaringan komputer untuk mendeteksi serangan yang terjadi, Lakukan pemantauan terhadap sistem jaringan komputer yang telah diimplementasikan IDS. Perhatikan apakah IDS dapat mendeteksi serangan dengan akurat dan memberikan notifikasi yang tepat

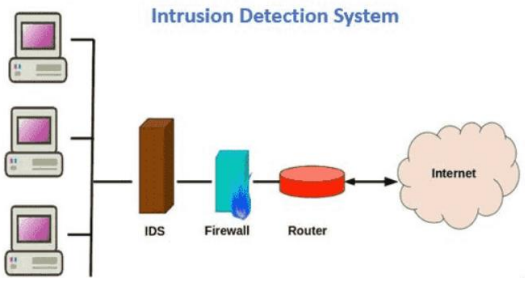
2.6 MANAJEMEN

Tahap ini merupakan sebuah langkah evaluasi secara keseluruhan mengenai kinerja dari Snort dan perangkat-perangkat pendukung lainnya, dalam hal ini tentu saja peneliti menjadikan hasil alert yang di berikan oleh snort sebagai acuan, apakah tingkat keamanan jaringan tersebut sesuai dengan keinginan client atau tidak, bila terjadi kekeliruan maka peneliti dan pihak PT Netkrida Tuah Cakrawala akan mencari kekeliruan tersebut dengan mengecek setingan tiap aplikasi terutama rules dari Snort, jika penelitian terlihat baik-baik saja dan sesuai dengan hasil yang diinginkan maka penelitian dinyatakan selesai.

3. HASIL DAN PEMBAHASAN

Dalam dunia keamanan jaringan, pendekatan yang digunakan dalam rule-based IDS dapat dibagi menjadi dua kategori utama(Cinderatama et al., 2022): Preemptory (pencegahan) dan Reactionary (reaksi). Pendekatan Preemptory pada IDS memfokuskan upayanya untuk mencegah ancaman sejak dini dengan secara aktif memeriksa dan menganalisis setiap paket yang melintasi jaringan. Begitu paket mencurigakan terdeteksi, program secara otomatis mengambil tindakan yang sesuai untuk menghentikan ancaman tersebut sebelum dapat menyebabkan kerusakan lebih lanjut.

Di sisi lain, pendekatan Reactionary pada rule-based IDS lebih bersifat responsif. Program hanya mengamati log atau catatan aktivitas jaringan, dan jika terdeteksi adanya paket mencurigakan, baru kemudian dilakukan tindakan sesuai dengan paket tersebut. Pendekatan ini cenderung lebih pasif, dengan fokus pada identifikasi dan penanganan ancaman setelah terjadi. Meskipun kedua pendekatan ini memiliki tujuan yang sama, yaitu melindungi jaringan dari ancaman keamanan, perbedaan utamanya terletak pada waktu pelaksanaan tindakan pencegahan, apakah dilakukan secara proaktif (Preemptory) atau responsif (Reactionary).



Gambar 4. Alur kerja IDS

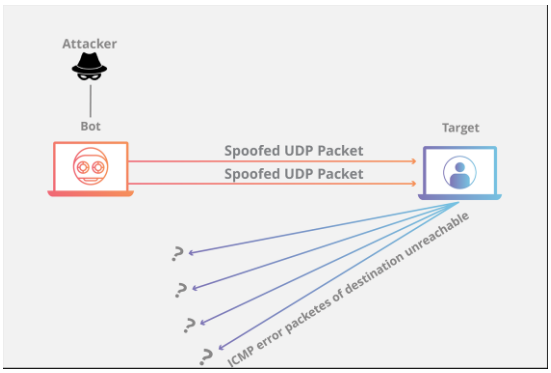
Dari gambar tersebut dapat dijelaskan bahwa rule-based IDS sangat bergantung pada penggunaan aturan-aturan yang telah ditentukan sebelumnya. Pertama-tama, IDS akan menganalisis lalu lintas jaringan dengan memeriksa setiap paket data yang melewati titik pemantauan. Aturan-aturan ini bersifat spesifik dan dirancang untuk mengenali pola-pola khas dari serangan atau aktivitas mencurigakan. Ketika suatu paket ditemukan sesuai dengan aturan yang telah ditentukan, IDS akan memicu alarm atau peringatan untuk memberitahu administrator jaringan atau sistem keamanan. Pendekatan ini memungkinkan IDS untuk secara efektif mendeteksi dan merespons serangan berdasarkan karakteristik yang telah didefinisikan sebelumnya.

Selain itu, rule-based IDS juga dapat memanfaatkan teknik pembelajaran mesin untuk meningkatkan ketepatan deteksi(Riza,

2022). Dalam hal ini, aturan-aturan dapat diperbarui secara otomatis berdasarkan pola-pola baru yang ditemukan melalui analisis data historis(Haryono et al., 2021). Dengan memanfaatkan kombinasi antara aturan-aturan statis dan pembelajaran mesin, rule-based IDS dapat memberikan tingkat keamanan yang lebih tinggi dan responsibilitas yang cepat terhadap serangan yang terus berkembang. Keseluruhan, kemampuan rule-based IDS untuk mengenali dan menanggapi ancaman secara cepat dan tepat membuatnya menjadi komponen penting dalam menjaga keamanan jaringan.

Dengan keberadaan IDS, sebuah topologi dapat dibangun untuk meningkatkan kinerja dalam aspek keamanan dan infrastruktur. IDS berperan penting dalam meningkatkan stabilitas sistem keamanan, membantu dalam mendeteksi potensi ancaman, dan merespons secara cepat terhadap serangan. Rincian kerja IDS diuraikan dalam kerangka kerja yang menggambarkan prosedur dan langkah-langkah yang diperlukan untuk membangun dan mengukur Intrusion Detection System.

Dalam skenario uji coba IDS berbasis Snort, percobaan simulasi akan dilakukan dengan mengeksplorasi serangan Denial of Service (DoS). Serangan ini bertujuan utama untuk menghentikan atau meniadakan layanan sistem atau jaringan komputer, mengakibatkan pengguna tidak dapat mengakses layanan tersebut. Contoh serangan denial of service yang diuji adalah melalui metode UDP (User Datagram Protocol) flooding. Serangan UDP flooding terjadi ketika jaringan diserang oleh paket-paket UDP yang mengalir ke port secara acak atau menyerang port tertentu yang rentan terhadap serangan.



Gambar 5. UDP Flooding

Beberapa parameter pada IDS yang digunakan dalam mendeteksi penyusup yang masuk diantaranya yaitu TCP, UDP, dan IP address. Beberapa perintah dasar yang digunakan dalam penelitian ini diantaranya:

```
alert tcp any any -> any any (msg:"UDP flood detected"; dsize>1000; sid:1000;)
```

Rule ini akan mendeteksi serangan UDP flood jika ukuran paket UDP yang diterima lebih besar dari 1000 byte. Sedangkan jika ada serangan UDP flood jika ukuran paket UDP yang diterima lebih besar dari 1000 byte dan jumlah paket UDP yang diterima dalam waktu 1 detik lebih besar dari 100, maka digunakan rule berikut:

```
alert tcp any any -> any any (msg:"UDP flood detected"; dsize>1000; threshold=100; sid:1001;)
```

Untuk mendeteksi serangan dengan menggunakan TCP, maka TCP Rule ini akan mendeteksi serangan TCP flood jika paket TCP yang diterima memiliki flag SYN:

```
alert tcp any any -> any any (msg:"TCP flood detected"; flags:S; sid:2000;)
```

Sedangkan untuk mendeteksi serangan TCP flood jika paket TCP yang diterima memiliki flag SYN dan jumlah paket TCP yang diterima dalam waktu 1 detik lebih besar dari 100, maka digunakan rule berikut:

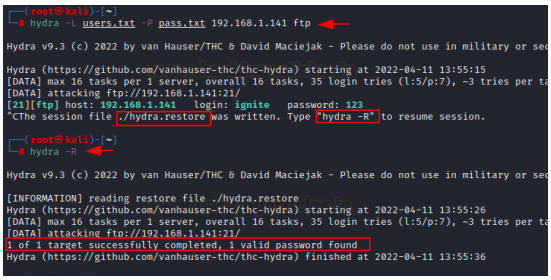
```
alert tcp any any -> any any (msg:"TCP flood detected"; flags:S; threshold=100; sid:2001;)
```

selain dari TCP dan UDP, penyerang juga kemungkinan memanfaatkan zombie IP address atau botnet. Zombie IP address merujuk pada alamat IP yang telah diretas atau dikendalikan oleh pihak yang tidak sah tanpa sepengetahuan pemiliknya. Zombie IP address sering kali terkait dengan komputer atau perangkat yang telah diambil alih oleh malware atau botnet. Dua rule yang dibangun ini akan mendeteksi zombie IP address jika paket TCP yang diterima memiliki flag SYN dan sumber IP-nya

```
alert tcp any any -> any any (msg:"Zombie IP address detected"; flags:S; src_ip=192.168.1.1; sid:3000;)

alert tcp any any -> any any (msg:"Zombie IP address detected"; flags:S; src_ip=192.168.1.1/24; sid:3001;)
```

Pengujian dilakukan dengan melakukan koneksi FTP pada server secara remote menggunakan tools hydra untuk melakukan serangan untuk mengambil username dan password (ditandai dengan warna merah).



Gambar 6. Log Hydra

Dari hasil pengujian yang dilakukan, dapat disimpulkan bahwa sistem yang dibuat berhasil mengolah output data dari IDS Snort dengan efektif dan mampu mengidentifikasi berbagai aktivitas yang dilakukan oleh intruder dalam upaya menyusup ke dalam sistem sesuai dengan aturan yang telah ditetapkan. Proses berikutnya melibatkan langkah pemblokiran terhadap IP address yang dianggap sebagai intruder, dan sistem secara otomatis memberikan laporan kepada administrator melalui jejaring sosial dan pemantauan web terkait upaya intrusi yang terdeteksi. Tabel 1 memberikan gambaran tentang kemampuan IDS dalam mengelola hasil output dari Snort untuk mendeteksi serangan dan melaksanakan proses pemblokiran beberapa IP yang telah diset sebagai zombie IP, dengan waktu dan perangkat yang berbeda menggunakan iptables.

Tabel 2. Pengetesan IDS

No	Zombie IP	Serangan Zombie	Respons IDS	Jeda (detik)
1	202.168.200.10	08:20:00	08:20:03	3
2	202.168.200.20	11:10:00	11:10:06	6
3	202.168.200.30	14:30:09	14:30:15	6
4	202.168.200.40	16:08:12	16:08:20	8
5	202.168.200.50	19:00:34	19:00:39	5
6	202.168.200.60	20:21:05	20:21:11	6
7	202.168.200.70	22:35:45	22:35:52	7
8	202.168.200.80	22:56:09	22:56:14	5
9	202.168.200.90	23:34:03	23:34:07	4
10	202.168.200.100	23:58:43	23:58:48	5

Tabel 1 memberikan gambaran waktu respons IDS terhadap serangan zombie IP pada berbagai kejadian. Terlihat bahwa respons IDS terhadap setiap serangan memiliki rentang waktu yang bervariasi, dengan jeda antara deteksi dan respons yang berkisar antara 3 hingga 8 detik. Pada beberapa kasus, respons IDS terjadi dengan waktu yang relatif cepat, seperti pada Zombie IP 202.168.200.10 dan 202.168.200.90 dengan jeda 3 dan 4 detik. Namun, terdapat kasus di mana respons IDS memakan waktu lebih lama, seperti pada Zombie IP 202.168.200.40 dengan jeda 8 detik.

Penting untuk mencermati waktu respons IDS ini karena dapat mempengaruhi efektivitas sistem dalam menanggapi ancaman. Waktu respons yang lebih cepat memungkinkan sistem untuk lebih proaktif dalam menghadapi serangan, sementara waktu respons yang lebih lama dapat meningkatkan risiko potensial dampak serangan terhadap sistem. Oleh karena itu, perlu diperhatikan faktor-faktor yang memengaruhi keterlambatan respons IDS dan diperbaiki untuk memastikan keamanan jaringan yang optimal. Selain itu, perlu dilakukan analisis lebih lanjut terkait efektivitas langkah-langkah respons yang diambil oleh IDS setelah deteksi, untuk memastikan bahwa tindakan pemblokiran dan laporan ke administrator dapat dilakukan dengan efisien.

4. SIMPULAN

Penelitian ini membuktikan bahwa IDS yang dibangun dengan menggunakan pendekatan rule-based, khususnya dengan menggunakan Snort, mampu secara efektif mendeteksi dan merespons serangan keamanan pada jaringan. Dengan mengimplementasikan aturan-aturan yang telah ditetapkan sebelumnya, sistem mampu mengenali pola-pola khas dari serangan seperti UDP flood, TCP flood, dan zombie IP address. Respons IDS terhadap serangan zombie IP

menunjukkan variasi waktu yang memerlukan perhatian lebih lanjut, dan hal ini dapat menjadi fokus perbaikan untuk meningkatkan kecepatan tanggapan sistem terhadap ancaman. Penerapan metode pemblokiran terhadap IP address yang dianggap sebagai zombie IP address juga menunjukkan potensi dalam meningkatkan keamanan jaringan. Laporan otomatis kepada administrator melalui jejaring sosial dan pemantauan web memberikan transparansi yang penting terkait dengan upaya intrusi yang terdeteksi. Oleh karena itu, keseluruhan penelitian ini menegaskan bahwa pendekatan rule-based IDS dapat digunakan dalam mengamankan jaringan, dengan penekanan pada respons cepat terhadap ancaman dan pemantauan yang efisien terhadap aktivitas mencurigakan.

5. DAFTAR PUSTAKA

Alfaeni, Z. D., & Fahriani, N. (n.d.). *Deteksi Serangan Ddos Pada Jaringan Rt / Rw-Net Desa Ketanen Dengan Metode Intrusion Detection System (IDS) Menggunakan Snort*. *x*, 28–34.

Amin, N. M., Hukum, F., & Wiraraja, U. (2023). Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime. *Prosiding Seminar Nasional Penelitian Dan Pengabdian Kepada Masyarakat*, *11*, 5–6.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11.

Cinderatama, T. A., Alhamri, R. Z., & Yunhasnawa, Y. (2022). Implementasi Metode K-Means, Dbscan, Dan Meanshift Untuk Analisis Jenis Ancaman Jaringan Pada Intrusion Detection System. *INOVTEK Polbeng - Seri Informatika*, *7*(1), 169. https://doi.org/10.35314/isi.v7i1.2336

Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. *Informasi Komputer Akuntansi Dan Manajemen*, *13*(2), 55–65.

Erdiyanto, R. P. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. *Jurnal Inovasi Global*, *1*(2), 71–79. https://jig.rivierapublishing.id/index.php/rv/index

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Haryani, P., & Raharjo, S. (2021). Manajemen Pada Jaringan Mikrotik Menggunakan Metode Hierarchical Token Bucket (Htb) Dan Keamanan Firewall Intrusion Detection System (IDS). *Jurnal Jarkom*, *09*(01), 1–9. https://ejournal.akprind.ac.id/index.php/jarkom/article/view/3669

Haryono, D., Zulianda, Y., Informasi, S., Amik Riau, S., Purwodadi Indah, J., & Informasi, T. (2021). Sistem Pendeteksian Serangan Jaringan Local Area Network (Lan) Menggunakan Algoritma Naive Bayes. *JOISIE Journal Of Information System And Informatics Engineering*, *5*(1), 1–8.

Hasanah, M., Marlina, T., Handoko, D., & Alamsyah, R. (2023). *Peran dan Tanggung Jawab Konsumen untuk Mencegah Praktik Penipuan dalam Transaksi Online dari Perspektif Hukum Perlindungan Konsumen Transaksi online semakin sering dilakukan oleh orang-orang baik di Indonesia maupun di dunia sebagai cara baru untuk melak*. *7*(1), 1–24.

Ilham, K. F. I., Alwi, E. I., & Fattah, F. (2023). Penerapan dan Analisis Network Security Snort Menggunakan Intrusion Detection System pada Serangan UDP Flood. *INFORMAL: Informatics Journal*, *8*(1), 94. https://doi.org/10.19184/isj.v8i1.34003

Jufri, M., & Heryanto. (2021). Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *5*(2), 98–108. https://doi.org/10.35145/joisie.v5i2.175

9

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce Data Breach and Identity Theft on E-Commerce. *CyberSecurity Dan Forensik Digital*, *3*(1), 7–13.

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. *Teknologi Informasi Dan Komunikasi*, 100–113.

Puntadheva, S. A., 2, R. Y. R. K., & J. Triyono. (2022). Perancangan Keamanan Jaringan Komputer Menggunakan Firewall Intrusion Detection System (Ids) Terhadap Serangan Brute Force Dan Implementasi Arp List. *Jurnal JARKOM*, *10*(2), 32–37.

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. *Jurnal Teknologi Informasi Dan Komunikasi*, *14*(2), 358–369. https://doi.org/10.51903/jtikp.v14i2.726

Riza, F. (2022). Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging. *Jurnal Sistim Informasi Dan Teknologi*, *5*, 7–9. https://doi.org/10.37034/jsisfotek.v5i1.161

Suhaemin, A., & Muslih. (2023). Karakteristik Cybercrime di Indonesia. *EduLaw : Journal of Islamic Law and Yurisprudance*, *5*(2), 15–26.

Surahman, F. (2023). Tantangan Dalam Menjaga Keamanan Data Official Statistics dari Serangan Cybercrime. *Jurnal Ilmiah Multidisiplin*, *1*(11), 904–907. https://doi.org/10.5281/zenodo.10371686