BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikasi Dengan Menggunakan Snort

M. Rafli Ramadhan[1], Joko Dwi Santoso[2], Sri Mulyatun[3]

[1,2,3] Teknik Komputer, Universitas Amikom Yogyakarta
[1,2,3] Jl. Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta

Coresponding Author e-mail: rafli.r@students.amikom.ac.id

Abstrak

Intrusion Detection System (IDS) adalah komponen penting dalam menjaga keamanan jaringan komputer. IDS bertugas untuk mengidentifikasi aktivitas mencurigakan atau serangan terhadap jaringan dan sistem komputer. Namun, efektivitas IDS dalam memberikan notifikasi kepada administrator tentang ancaman keamanan dapat ditingkatkan dengan memanfaatkan media komunikasi yang lebih efisien dan real-time. Penelitian ini bertujuan untuk mengimplementasikan IDS menggunakan perangkat lunak Snort dan mengintegrasikannya dengan jejaring sosial sebagai media notifikasi. Metode yang digunakan melibatkan instalasi dan konfigurasi Snort pada jaringan, pengumpulan data lalu lintas, analisis data menggunakan aturan Snort, dan pengiriman notifikasi melalui jejaring sosial. Media jejaring sosial dipilih karena memiliki kecepatan dan aksesibilitas yang baik, memungkinkan administrator untuk segera merespons ancaman keamanan. Hasil penelitian menunjukkan bahwa integrasi Snort dengan jejaring sosial dapat meningkatkan respons terhadap ancaman keamanan dengan memberikan notifikasi secara real-time kepada administrator. Hasil penelitian ini diharapkan dapat menjadi landasan untuk pengembangan lebih lanjut dalam bidang keamanan jaringan komputer.

Kata kunci: *IDS, Snort, Telegram, Keamanan Jaringan, Jejaring Sosial*

Abstract

Intrusion Detection System (IDS) is an important component in maintaining computer network security. IDS is tasked with identifying suspicious activity or attacks on computer networks and systems. However, the effectiveness of IDS in notifying administrators about security threats can be improved by utilizing more efficient and real-time communication media. This research aims to implement IDS using Snort software and integrate it with social networks as a notification medium. The methods used involve installing and configuring Snort on the network, collecting traffic data, analyzing data using Snort rules, and sending notifications via social networks. Social networking media was chosen because it has good speed and accessibility, allowing administrators to respond promptly to security threats. The results show that Snort's integration with social networks can improve response to security threats by providing real-time notifications to administrators. The results of this research are expected to be the foundation for further development in the field of computer network security.

Keywords: *IDS, Snort, Telegram, Network Security, Social Network*

1. Pendahuluan

Pesatnya perkembangan teknologi di era revolusi industri 4.0 juga harus diimbangi dengan kemampuan system administrator dalam mengola sistem yang sedang dibangun. Selain dapat

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

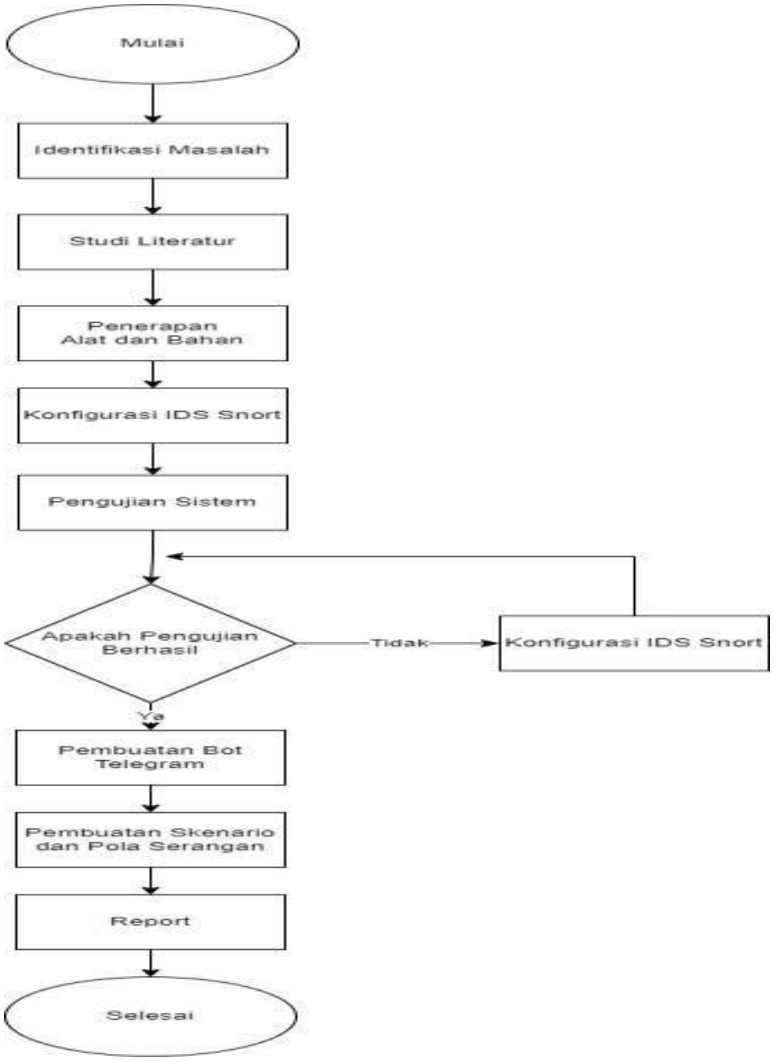
memberikan informasi yang fleksibel dan terkini, layanan informasi juga harus dapat diandalkan dan aman. Sistem komunikasi dan penyebaran informasi yang tidak lagi dibatasi oleh tempat dan waktu, telah menjadi peluang bagi para pelaku kejahatan di dunia internet, atau biasa disebut dunia cybercrime. Oleh karena itu, faktor keamanan jaringan menjadi parameter penting yang harus dipersiapkan dengan baik untuk menghidari upaya ilegal oleh oknum yang tidak bertanggung jawab untuk mencuri data atau merusak sistem yang ada. Berbagai serangan yang sering mengancam jaringan, seperti virus, sniffing, spoofing merupakan resiko yang harus dihadapi oleh administrator sistem setiap hari. Selain itu, brute force, scanning, malware, dan Denial of Services (DOS). Sistem Deteksi Intrusi (IDS) adalah perangkat lunak atau sistem perangkat keras yang beroperasi secara otomatis untuk memantau kejadian di dalam jaringan komputer dan dapat menganalisis isu-isu keamanan jaringan. Sebuah IDS dapat diartikan sebagai alat, metode, atau sumber daya yang memberikan bantuan dalam mengidentifikasi dan melaporkan aktivitas di dalam jaringan komputer[1]. Snort adalah suatu perangkat pemasangan paket pada sistem operasi Linux, yang fungsinya utamanya adalah untuk mengidentifikasi kehadiran ancaman (threats). Snort memiliki kemampuan untuk menganalisis paket data yang bergerak melalui jaringan secara real-time dan menghasilkan catatan dalam bentuk basis data. Snort menjadi salah satu contoh dari jenis sistem deteksi intrusi (IDS) yang termasuk dalam kategori sistem deteksi intrusi berbasis jaringan (NIDS), suatu program sistem yang mampu menemukan tanda-tanda adanya intrusi di dalam jaringan komputer[2]. Telegram adalah aplikasi messenger yang akan membantu pihak administrator untuk memonitoring jaringan lebih mudah. Karena setiap serangan yang terdeteksi oleh Snort akan memberikan alert ke Telegram dan di terima oleh pihak administrator. Dari Telegram akan terlihat jenis serangan dan status serangan berbahaya atau tidak bagi administrator[3]. Keamanan data sangat penting dalam lingkungan jaringan, pemantauan sistem 24jam penuh tidak mungkin dilakukan jika harus dilakukan secara manual. Perlu bantuan sistem pengganti manusia untuk pemantauan terus menerus, yang diharapkan dapat mendeteksi dan mencegah serangan terhadap jaringan atau server. Intrusion Detection System (IDS) menjadi peluang bagi administrator sistem untuk mendeteksi dan mencegah aktivitas yang mencurigakan.Snort adalah sebuah aplikasi yang bisa digunakan sebagai Intrusion Detection System (IDS) yang berfungsi untuk mendeteksi adanya serangan atau sebuah aktifitas yang mencurigakan. Telegram disini berfungsi sebagai media notifikasi atau pemberitahuan ke sistem deteksi serangan dan mencatat aktivitasnya. Adapun tujuan penelitian ini adalah 1) Mendeteksi adanya serangan ICMP, SSH, Nmap, dan SYN Flood menggunakan IDS, dan 2) Melakukan pengujiankecepatan IDS dalam mendeteksi adanya serangan ICMP, SSH, Nmap, dan SYN Flood.

2. Metode Penelitian

Berikut merupakan alur Implementasi Intrusion Detection System (IDS) menggunakan jejaring sosial sebagai media notifikasi dengan menggunakan snort disajikan pada Gambar 1. Gambar 1 menyajikan, identifikasi masalah merupakan langkah pertama dalam proses penelitian. Setelah permasalahan teridentifikasi, langkah selanjutnya menganalisa serta menerapkan sistem keamanan jaringan IDS menggunakan Snort, dengan notifikasi melalui telegram pada web server.Studi Literatur digunakan sebagai acuan untuk memahami konsep dasar dalam menjalankan implementasi, perancangan, dan pengujian pada berbagai tahap penelitian. Landasan teori yang diperlukan seba gai penopang studi ini melibatkan konsep OpenSource, Intrusion Detection System (IDS), Snort IDS, Virtual Private Server (VPS), dan tools snort. Kedua, penerapan alat dan bahan dalam implementasi intrusion detection system menggunakan jejaring sosial telegram dengan menggunakan snort menggunakan sejumlah software dan hardware yang akan digunakan untuk menguji dan menerapkan sistem keamanan. Ketiga, konfigurasi IDS Snort pada pelaksanaan analisis keamanan dengan Snort dan notifikasi melalui jejaring sosial telegram pada web server melibatkan serangkaian langkah untuk mengaktifkan dan menyusuaikan Snort agar dapat mendeteksi serangan yang berhubungan dengan aplikasi web yang sedang dijalankan. Keempat, pengujian Sistem digunakan untuk memastikan intrusion detection system berfungsi

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

dengan benar dan mampu mendeteksi serangan dengan tepat. Kelima, pembuatan Bot Telegram digunakan untuk menambah efektifitas dalam penggunaan intrusion detection system agar lebih efisien. Keenam, pembuatan skenario dan pola serangan bertujuan untuk menguji respons dan efektifitas intrusion detection system dalam mendeteksi berba gai jenis serangan yang mungkin terjadi. Terakhir, Report adalah penulisan hasil dari proses pengujian sistem intrusion detection system menggunakan jejaring sosial telegram dengan menggunakan snort.



Gambar 1. Alur Penelitian

2.1. Analisis Keamanan Jaringan

Tujuan utama keamanan jaringan komputer adalah menjaga kerahasiaan, integritas, dan ketersediaan data serta memastikan bahwa jaringan komputer dan sistem yang terkoneksi aman dari serangan.

- Beberapa aspek penting dalam keamanan jaringan komputer meliputi[4]:
- Rahasia (Confidentiality): menjaga kerahasiaan informasi sensitif .
- Integritas (Integrity): memastikan data dan sistem tidak mengalami perubahan yang tidak sah.
- Ketersediaan (Availability): memastikan jaringan komputer tetap tersedia dan dapat diakses.
- Autentikasi (Authentication): verifikasi identitas pengguna.

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

- Otorisasi (Authorization): mengatur izin dan hak akses pengguna.
- Keamanan Fisik (Physical Security): melindungi perangkat keras fisik dari akses yang tidak sah

2.2. IDS

Sistem Deteksi Intrusi (*IDS*) adalah perangkat lunak atau sistem perangkat keras yang beroperasi secara otomatis untuk memantau kejadian di dalam jaringan komputer dan dapat menganalisis isu-isu keamanan jaringan. Sebuah *IDS* dapat diartikan sebagai alat, metode, atau sumber daya yang memberikan bantuan dalam mengidentifikasi dan melaporkan aktivitas di dalam jaringan komputer. Sebenarnya, *IDS* tidak mendeteksi penyusup, melainkan mengidentifikasi lalu lintas jaringan yang tidak wajar, sehingga langkah-langkah awal yang dilakukan oleh penyerang dapat dikenali. Dengan demikian, administrator jaringan dapat mengambil tindakan pencegahan dan bersiap menghadapi potensi serangan yang mungkin terjadi[1].

2.3. Snort

Snort adalah suatu perangkat pemasangan paket pada sistem operasi Linux, yang fungsinya utamanya adalah untuk mengidentifikasi kehadiran ancaman (threats). Snort memiliki kemampuan untuk menganalisis paket data yang bergerak melalui jaringan secara real-time dan menghasilkan catatan dalam bentuk basis data[2]. Snort berfungsi sebagai perangkat yang digunakan untuk mendeteksi dan juga mencegah, saat sebuah paket data dalam lalu lintas jaringan diidentifikasi sebagai ancaman atau terdeteksi sebagai ancaman. Di dalam Snort terdapat pula peraturan (mirip dengan firewall) yang berperan dalam pendeteksian ancaman dengan cara mengawasi setiap data lalu lintas yang bergerak dalam jaringan. Aplikasi Snort ini diterapkan menggunakan himpunan peraturan (set peraturan) dengan format aturan khusus, yang memungkinkan sistem Linux menjalankan aturan-aturan untuk mengenali pola serangan yang dilakukan oleh penyerang. Ketika pola perilaku yang tidak wajar terdeteksi, Snort akan memberikan peringatan[2].

2.4. Ancaman Serangan

- Distributed Denial of Service (DDoS) terjadi ketika penyerang berhasil menggabungkan beberapa layanan sistem dan menggunakannya sebagai pusat untuk menyebarkan serangan terhxadap korban[5].
- SYN flooding adalah upaya untuk menghamburkan sinyal SYN kepada sistem yang menggunakan protokol TCP/IP dalam inisiasi sesi komunikasi[5].
- Nmap (Port Scanning) merupakan ancaman yang cukup serius bagi suatu sistem jaringan komputer, dan menjadi hal yang sangat menguntungkan bagi para attacker. Dengan Port Scanning, attacker mendapatkan informasi-informasi berharga yang dibutuhkan dalam melakukan serangan. Dengan kata lain, melakukan Port Scanning ialah untuk mengidentifikasi port-port yang terbuka, dan mengenali OS (Operating System) target[5].

2.5. Firewall

Firewall adalah sebuah perangkat yang memiliki fungsi untuk memeriksa dan mengontrol paket data yang masuk dan keluar dari suatu jaringan. Dengan kemampuannya dalam menentukan apakah paket data tersebut diperbolehkan atau tidak, *firewall* berperan penting dalam melindungi jaringan dari serangan yang datang dari internet. Selain menjaga keamanan jaringan, *firewall* juga digunakan untuk melindungi komputer pengguna atau *host* (sebuah komputer *individual*), dalam hal ini dikenal sebagai *host firewall*[6].

2.6. VMWare

VMWare adalah sebuah aplikasi *open-source* yang terkait dengan teknologi *virtualisasi*. *Virtualisasi* ini merujuk pada kemampuan menjalankan sistem operasi lain secara mandiri di atas sistem operasi utama[7]. Dengan menggunakan *VMWare*, pengguna dapat memiliki beberapa

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

komputer *virtual* dengan sistem operasi yang dapat disesuaikan sesuai keinginan, misalnya Windows, Linux, macOS X, dan sebagainya.[8].

2.7. Ubuntu

Ubuntu adalah sebuah sistem operasi berbasis sumber terbuka yang dikembangkan oleh Linux dengan basis Debian dan didistribusikan sebagai perangkat lunak bebas. Nama Ubuntu berasal dari filosofi Afrika Selatan yang mengartikan "kemanusiaan kepada sesama". Ubuntu dirancang untuk penggunaan pribadi, tetapi juga memiliki versi *server* yang telah digunakan secara luas. Proyek Ubuntu didukung secara resmi oleh *Canonical Ltd*. Sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan, *Mark Shuttleworth*. Tujuan dari distribusi Linux Ubuntu adalah untuk menghadirkan semangat filosofi Ubuntu ke dunia perangkat lunak. Ubuntu adalah sebuah sistem operasi lengkap yang berbasis Linux, tersedia secara gratis, dan mendapatkan dukungan baik dari komunitas maupun tenaga ahli profesional[9].

2.8. Kali Linux

Kali Linux merupakan salah satu distro Linux yang berasal dari turunan Debian yang dikembangkan dengan fokus sebagai sistem operasi yang digunakan untuk melakukan pengujian keamanan jaringan[7].

2.9. Telegram Bot-API

Telegram *Bot-API* adalah sebuah perangkat lunak yang memungkinkan interaksi antara *bot* dengan pengguna (administrator). *Bot* ini memiliki fokus khusus pada keamanan jaringan dan memiliki kemampuan untuk mengirim perintah dari jarak jauh serta memberikan peringatan terhadap serangan[10]. *Bot API* ini merupakan antarmuka berbasis *HTTP* yang menghubungkan *bot* yang dikembangkan oleh para pengembang dengan sistem Telegram[11]. Salah satu keunggulan Telegram adalah adanya landasan untuk menggunakan *Application Programming Interface* (*API*) yang dapat diakses oleh masyarakat umum. Salah satu *API* yang tersedia adalah fitur *bot*. *Bot* Telegram semakin populer dan banyak digunakan saat ini[11].

2.10. Alat dan bahan

Diperlukan beberapa hardware dan software yang akan digunakan untuk membantu kelancaran penelitian, adapun alat yang diperlukan diantaranya:

Tabel 1. Spesifikasi hardware

No	Jenis	Spesifikasi
1.	*Processor*	AMD Ryzen 52400G
2.	*RAM*	Trident Z DDR4-3200 CL14-14-14-34 1.35V 16GB (2x8GB)
3.	*Storage*	BULLDOZER SSD 240GB SATA BX250
4.	*Motherboard*	msi B450M GAMING PLUS
5.	*Graphics Card*	AMD Radeon RX5700 8GB
6.	*PSU*	MSI MPG A650GF
7.	*Display*	LED SPC SM- 19HD 19” Black

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

Tabel 2. Spesifikasi software

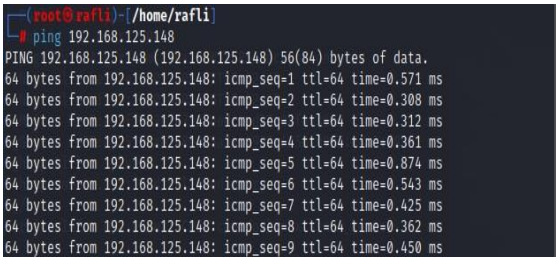
No	Jenis	Spesifikasi
1.	*Processor*	AMD Ryzen 52400G
2.	*RAM*	Trident Z DDR4-3200 CL14-14-14-34 1.35V 16GB (2x8GB)
3.	*Storage*	BULLDOZER SSD 240GB SATA BX250
4.	*Motherboard*	msi B450M GAMING PLUS
5.	*Graphics Card*	AMD Radeon RX5700 8GB
6.	*PSU*	MSI MPG A650GF
7.	*Display*	LED SPC SM- 19HD 19” Black

3. Hasil dan Pembahasan

Hasil Install Snort Penulis menggunakan Snort versi 3.1.18.0 untuk melakukan pengujian.

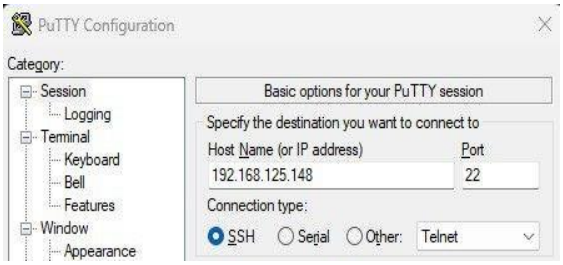
Gambar 2. Install snort

Hasil Pengujian ICMP, Dalam melakukan ICMP ke server, penulis menggunakan Kali Linux. Dengan cara melakukan ping IP server ubuntu dengan mengetikkan ping 192.168.125.148.



Gambar 3. Pengujian icmp

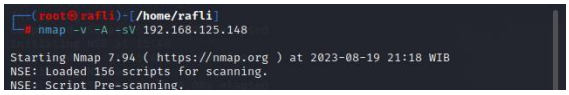
Hasil melakukan Login SSH Melalui PuTTY, dengan membuka aplikasi PuTTY penulis mengisi form hostname dengan alamat IP dari server Ubuntu 192.168.125.148 dan di port 22 tempat layanan SSH.



Gambar 4. Pengujian ssh

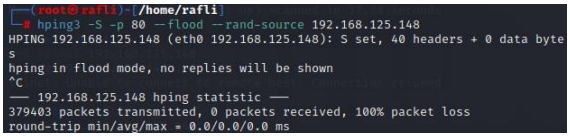
Hasil Melakukan Serangan Nmap, dalam melakukan serangan Nmap ke server, penulis menggunakan perintah nmap -v -A -sV 192.168.125.148

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….



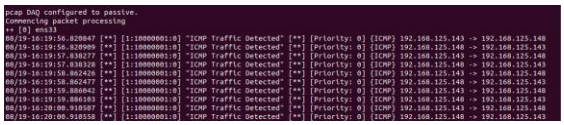
Gambar 5. Pengujian nmap

Hasil Melakukan Serangan SYN Flood, dalam melakukan serangan SYN Flood ke server dengan menggunakan Kali Linux, penulis menggunakan tool hping3.



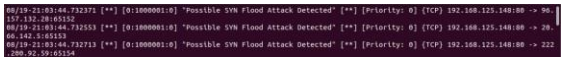
Gambar 6. Pengujian syn flood

Hasil Pengecekan Log Snort Ubuntu, Pengecekan pada log Snort Ubuntu dilakukan untuk melihat detail data mengenai serangan yang terjadi. Untuk melihat log snort maka penulis mengetik perintah sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules \ -i ens33 -A alert_fast -s 65535 -k none.



Gambar 7. *Log* snort icmp

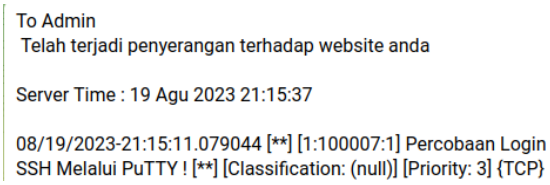
Gambar 8. *Log* snort nmap



Gambar 9. *Log* snort syn flood

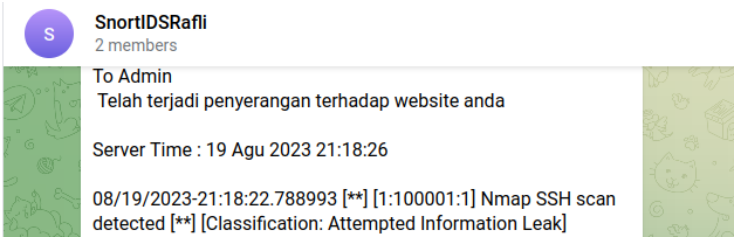
Hasil Pengecekan Notifikasi Telegram, Pada saat penulis menjalankan serangan ICMP, SSH, Nmap dan SYN Flood, maka saat itu juga notifikasi telegram masuk. Hal tersebut dapat dilihat pada gambar berikut.

Gambar 10. Notifikasi icmp snort telegram

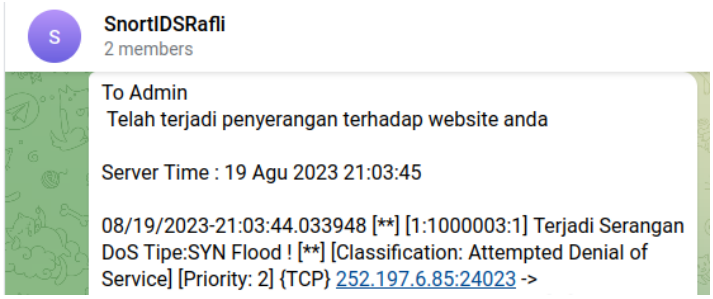


Gambar 11. Notifikasi ssh snort telegram

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….



Gambar 12. Notifikasi nmap telegram



Gambar 13. Notifikasi syn flood telegram

3.1. Hasil Deteksi Serangan

Tabel 3. Hasil akurasi serangan

No	Jenis Serangan	Port	Waktu		Jumlah Serangan
			Awal Serangan	Terdeteksi	Terkirim	
1.	ICMP	138	15:43:37	15:43:37	15:43:37	10
2.	SSH	22	21:15:37	21:15:37	21:15:37	10
3.	Nmap	80	21:18:40	21:18:40	21:18:40	10
4.	SYN Flood	80	21:03:45	21:03:45	21:03:45	10

Dari hasil pengujian sistem diambil kesimpulan yang tertera pada tabel diatas, sehingga menunjukkan Sistem dapat mendeteksi adanya serangan yang dilakukan oleh attacker kemudian mengirimkan notifikasi melalui aplikasi Telegram. Pendeteksian serangan telah sesuai dengan aturan yang dibuat mulai dari ICMP, SSH, Nmap, dan SYN Flood telah sesuai dengan hasil yang diharapkan.

Tabel 4. Hasil pengujian sistem

No	Jenis Serangan	Hasil Pengujian	Kesimpulan
1.	ICMP	Terdeteksi	Berhasil
2.	SSH	Terdeteksi	Berhasil
3.	Nmap	Terdeteksi	Berhasil
4.	SYN Flood	Terdeteksi	Berhasil

Dari tabel diatas hasil pengujian serangan yang didapatkan, penyerang melakukan empat pengujian sistem ICMP, SSH, Nmap, dan SYN Flood untuk penyerangan tersebut menggunakan sistem operasi kali linux untuk menyerang server IDS Snort, penulis mendapatkan empat tipe

serangan yang berbeda mulai dari ICMP, SSH, Nmap, dan SYN Flood. Pada status monitoring didalam server IDS Snort mendeteksi empat serangan yang masuk artinya semua serangan yang masuk itu sukses dan telah terdeteksi oleh Snort, setelah mendapatkan serangan yang masuk dilakukan integrasi notifikasi pengiriman melalui telegram administrator bisa mendapatkan notifikasi tersebut menggunakan smartphone atau laptop. Dari simulasi pengujian sistem keamanan IDS Snort dapat di ambil kesimpulan, sistem akan menunjukkan adanya serangan yang akan dideteksi oleh IDS Snort jika terjadinya penyerangan terhadap server IDS Snort secara otomatis akan mengirimkan notifikasi melalui telegram, pendeteksian serangan yang telah dilakukan sesuai dengan aturan yang di buat mulai dari ICMP, SSH, Nmap dan SYN Flood.

4. Kesimpulan dan saran

Intrusion Detection System (IDS) mampu mendeteksi adanya serangan ICMP, SSH, Nmap dan SYN Flood. IDS (Intrusion Detection System) memiliki kemampuan mendeteksi serangan ICMP, SSH, Nmap, dan SYN Flood dalam waktu sangat cepat (1 detik), tanpa jeda waktu dalam pemantauan, dan mengirimkan laporan secara otomatis mela lui telegram. Kedepan akan lebih dipertimbangkan dalam mengintegrasikan IDS dengan perangkat keamanan lainnya seperti firewall atau sistem keamanan lainnya untuk meningkatkan pertahanan keseluruhan jaringan. Selanjutnya akan dilakukan penelitian dan pembaruan terkait dengan ancaman terbaru dalam dunia siber dan selalu perbarui aturan IDS Anda untuk mencerminkan perubahan ini. Mempertimbangkan integrasi sistem IDS dengan platform lain untuk pemantauan keamanan secara komprehensif. Snort dapat dikombinasikan dengan software intrusi yang lainnya seperti snorby dan barnyard,Kibana PFSanse dll.

PUSTAKA

[1] H. Suhendi and W. D. Cahyo, "Perancangan Dan Implementasi Keamanan Jaringan Menggunakan Snort Sebagai Intrusion Prevention System (Ips) Pada Jaringan …," *Naratif J. Nas. Ris. …*, vol. 03, no. 02, pp. 60–68, 2021, [Online]. Available: https://naratif.sttbandung.ac.id/index.php/naratif/article/view/137%0Ahttps://naratif.sttbandung.ac.id/index.php/naratif/article/download/137/71.

[2] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu," *Netw. Eng. Res. Oper.*, vol. 6, no. 1, p. 11, 2021, doi: 10.21107/nero.v6i1.190.

[3] D. Kusuma, U. Darussalam, and D. Hidayatullah, "Implementasi Monitoring Jaringan Melalui Aplikasi Sosial Media Telegram Dengan Snort," *J I M P - J. Inform. Merdeka Pasuruan*, vol. 5, no. 1, pp. 6–9, 2020, doi: 10.37438/jimp.v5i1.242.

[4] E. Utami and T. Informasi, "Analisis Keamanan Jaringan Komputer Menggunakan Teknik Intrusion Detection System (IDS) pada Lingkungan Perusahaan," vol. 3, no. 6, pp. 2023–2024, 2023.

[5] U. M. D. E. C. D. E. Los, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title."

[6] J. D. Santoso, "Analisis Perbandingan Metode Queue Pada Mikrotik," *Pseudocode*, vol. 7, no. 1, pp. 1–7, 2020, doi: 10.33369/pseudocode.7.1.1-7.

[7] R. R. Adha, M. F. Rizal, and S. J. I. Ismail, "Membangun Sistem Keamanan Jaringan Berbasis Firewall Dan Ids Menggunakan Tools Opnsense," *eProceedings …*, vol. 7, no. 6, pp. 2846–2856, 2021, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034/16747.

[8] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," *J. Infra*, vol. 10, no. 1, pp. 1–6, 2022, [Online]. Available: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/12033.

[9] G. Tambunan and M. IGN, "Implementasi Keamanan Ids / Ips Dengan Snort Dan IP Tables pada Server," *Semin. Nas. Mhs. Ilmu Komput. dan Apl. Jakarta-Indonesia, 28 Januari 2020 IMPLEMENTASI*, pp. 10–16, 2020.

BHATARA: Jurnal Multidisiplin
Vol. 1, No. 1, Januari 2024, pp. 31~ 40
EISSN: …….

[10] D. D. Mahendra and F. S. Mukti, "Sistem Deteksi dan Pengendalian Serangan Denial of Service pada Server Berbasis Snort dan Telegram-API," *Techno.Com*, vol. 21, no. 3, pp. 511–522, 2022, doi: 10.33633/tc.v21i3.6466.

[11] G. Citra Lenardo, "Pemanfaatan Bot Telegram Sebagai Media Informasi Akademik di STMIK Hang Tuah Pekanbaru (Utilization of Telegram Bot as Academic Information Media at STMIK Hang Tuah Pekanbaru)," *J. Teknol. Inf. dan Multimed.*, vol. 1, no. 4, pp. 351–357, 2020.