Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 4 October 2024, pp: 1614-1623
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Implementation of IDS on Computer Networks Using Snort Based on Telegram Chatbot

Implementasi IDS pada Jaringan Komputer Menggunakan Snort Berbasis Chatbot Telegram

Ferry Ardiyansyah[1*], Kiki Setiawan[2], Nandang Sutisna[3]

[1,2,3]Program Studi Teknik Informatika,
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Indonesia

E-Mail: [1]ardiyansyahferry@gmail.com,
[2]ki2djoaz@stikomcki.ac.id, [3]nandang.sutisna@stikomcki.ac.id,

Received Jul 17th 2024; Revised Aug 26th 2024; Accepted Oct 5th 2024
Corresponding Author: Ferry Ardiyansyah

Abstract

In this digital era, information security and computer network protection are crucial. Internet usage in Indonesia reached 79.50% of the population in 2024, accompanied by increasing cyber threats such as Ping of Death (POD), Nmap scanning, and DDoS. PT Tiga Kawan Sertifikasi faces challenges in managing network security. This research aims to implement an attack detection system using Snort integrated with a Telegram chatbot for real-time notifications. The research method includes configuring an Ubuntu server as an IDS with Snort and using a Telegram chatbot as the notification medium. Testing was conducted with a pentest scenario using a Kali Linux server. The test results show Snort detecting Ping of Death attacks in 4 seconds, Nmap scanning in 3 seconds, and DDoS in 2 seconds. The system successfully sends alerts to the Telegram group, effectively and efficiently optimizing the network security of PT Tiga Kawan Sertifikasi. Overall, the results indicate that this solution can provide better protection against cyber threats and allow quick response to security incidents. Additionally, the system facilitates network administrators in monitoring and handling attacks in real-time, enhancing the company's network resilience.

Keyword: Attack Detection, Computer Network, Network Security, Snort, Telegram Chatbot

Abstrak

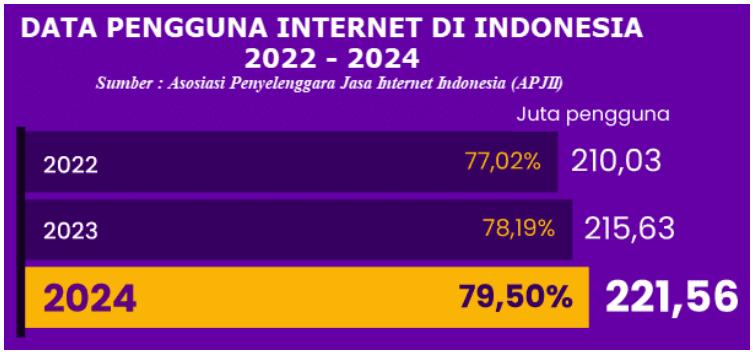
Pada era digital ini, keamanan informasi dan perlindungan jaringan komputer sangat penting. Penggunaan internet di Indonesia mencapai 79,50% dari populasi pada tahun 2024, disertai meningkatnya ancaman siber seperti Ping of Death (POD), Nmap scanning, dan DDoS. PT Tiga Kawan Sertifikasi menghadapi tantangan dalam mengelola keamanan jaringan. Penelitian ini bertujuan mengimplementasikan sistem deteksi serangan menggunakan Snort yang terintegrasi dengan chatbot Telegram untuk notifikasi real-time. Metode penelitian mencakup konfigurasi server Ubuntu sebagai IDS dengan Snort dan penggunaan chatbot Telegram sebagai media notifikasi. Pengujian dilakukan dengan skenario pentest menggunakan server Kali Linux. Hasil pengujian menunjukkan Snort mendeteksi serangan Ping of Death dalam 4 detik, Nmap scanning dalam 3 detik, dan DDoS dalam 2 detik. Sistem berhasil mengirimkan alert pada grup Telegram, mengoptimalkan keamanan jaringan PT Tiga Kawan Sertifikasi secara efektif dan efisien. Keseluruhan hasil menunjukkan bahwa solusi ini dapat memberikan perlindungan yang lebih baik terhadap ancaman siber dan memungkinkan respons cepat terhadap insiden keamanan. Selain itu, sistem ini mempermudah administrator jaringan dalam memantau dan menangani serangan secara real-time, meningkatkan ketahanan jaringan perusahaan.

Kata Kunci: Chatbot Telegram, Deteksi Serangan, Jaringan Komputer, Keamanan Jaringan, Snort

1. PENDAHULUAN

Dalam era digital yang berkembang pesat saat ini, keamanan informasi menjadi hal yang sangat penting, terutama dalam konteks jaringan komputer. Memastikan keamanan data dan privasi menjadi prioritas utama dalam menghadapi tantangan-tantangan cyber yang semakin kompleks. Pemanfaatan teknologi informasi di semua sektor sangat vital di zaman sekarang, termasuk dalam hal penggunaan internet. Saat ini, dalam kehidupan sehari-hari, berbagai bidang, profesi, dan sektor bergantung pada internet. Sehingga setiap tahunnya

berdasarkan data dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), penggunaan internet di Indonesia pada tahun 2024 mengalami peningkatan dari setiap tahun sebelumnya.



Gambar 1. Pengguna Internet diindonesia 2022-2024 [1]

Pada tahun tersebut, jumlah total pengguna internet mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia pada tahun 2023. Survei penetrasi internet yang dilakukan oleh APJII pada tahun 2024 menunjukkan bahwa tingkat penetrasi internet di Indonesia mencapai 79,50%, mengalami peningkatan sebesar 1,4% dibandingkan dengan periode sebelumnya pada tahun 2023 [2],[1]. Sehingga dengan bertambah nya penggunaan internet maka bertambah pula tingkat kejahatan di internet tersebut. Kejahatan siber tidak hanya berpotensi merusak data dan informasi pribadi, tetapi juga dapat mengancam infrastruktur dan stabilitas keamanan nasional suatu negara. Serangan siber, atau yang dikenal sebagai cyberattack, merupakan tindakan yang dilakukan oleh para pelaku kejahatan siber menggunakan satu atau lebih komputer untuk menyerang satu atau beberapa komputer atau jaringan [3],[4]. Kondisi ini menjadi perhatian serius bagi individu, perusahaan, dan pemerintah. Menurut laporan Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami 370,02 juta serangan siber pada tahun 2022 [5]. Secara khusus, mayoritas serangan siber pada tahun tersebut berasal dari dalam negeri, yakni sebanyak 84,86 juta [6]. Selain itu, terdapat 80,36 juta serangan siber yang berasal dari India dan 27,99 juta dari Bangladesh. Dilihat dari sektor yang menjadi target, sektor administrasi pemerintahan mengalami jumlah serangan paling banyak, mencapai 284,09 juta kasus pada tahun 2022 [7].

Dengan demikian, keamanan jaringan internet menjadi sangat penting untuk menjaga validitas dan integritas data, serta untuk menjamin ketersediaan layanan bagi penggunanya [8]. Hal ini bertujuan agar data atau sistem jaringan tidak terganggu atau dirusak oleh penyusup. Beberapa serangan yang sering terjadi meliputi port scanning dan Distributed Denial of Service (DDOS) Port scanning merupakan serangan yang mengeksplorasi kelemahan dalam sistem jaringan komputer tersebut. Sementara itu, Distributed Denial of Service (DDOS) [9] merupakan serangan yang mengirimkan permintaan secara berulang ke server dengan tujuan membuat server menjadi sibuk sehingga menyebabkan kerusakan pada layanan yang disediakan oleh server tersebut [10],[11].

Intrusion Detection System (IDS) adalah aplikasi perangkat lunak yang digunakan untuk mendeteksi aktivitas atau lalu lintas yang tidak wajar dalam sebuah sistem atau jaringan [12],[13]. Snort IDS adalah salah satu jenis IDS yang bersifat open source dan telah menjadi standar IDS di industri. Dengan demikian, Snort merupakan sistem yang mampu mendeteksi serangan jaringan secara real-time dan memberikan peringatan (alert) terhadap serangan jaringan tersebut [14], [15].

Pada penelitian terdahulu oleh Adhitya Nugraha dan Dinda Aulia Gustian, masalah yang diangkat adalah ancaman malware Dridex, yang mampu mencuri data kredensial perbankan dan informasi pribadi keuangan melalui spam email dan teknik rekayasa sosial. Penelitian ini mengembangkan dan mengimplementasikan 12 rules dalam Snort berdasarkan signature Dridex yang dianalisis dari dataset lalu lintas jaringan. Hasil penelitian menunjukkan bahwa Snort efektif dalam mendeteksi Dridex dengan tingkat deteksi yang sangat baik, terutama recall yang mencapai 100% [6].

Selanjutnya, penelitian oleh Zulhelm Dwi Alfaeni dan Nuniek Fahriani membahas masalah pada jaringan swadaya masyarakat (RT/RW net), yang minim pengawasan dan belum memiliki sistem pendeteksi serangan. Penelitian ini mengimplementasikan Snort sebagai IDS untuk mendeteksi serangan ICMP, Nmap, dan DDoS. Hasil penelitian menunjukkan bahwa Snort efektif dalam mendeteksi serangan dan membantu administrator jaringan dalam mengambil tindakan [16].

Lalu pada Penelitian lainnya oleh Rizkial Achmad, Evanita Veronica Manullang, dan Emha Rizal Sanmas menyoroti kerentanan jaringan komputer terhadap serangan DDoS, Port Scanning, dan SQL Injection. Penelitian ini merancang sistem deteksi jaringan menggunakan Snort yang terintegrasi dengan SMS gateway untuk notifikasi serangan secara real-time. Hasil penelitian menunjukkan bahwa Snort efektif sebagai sistem deteksi dan pemberi notifikasi serangan secara real-time [17].

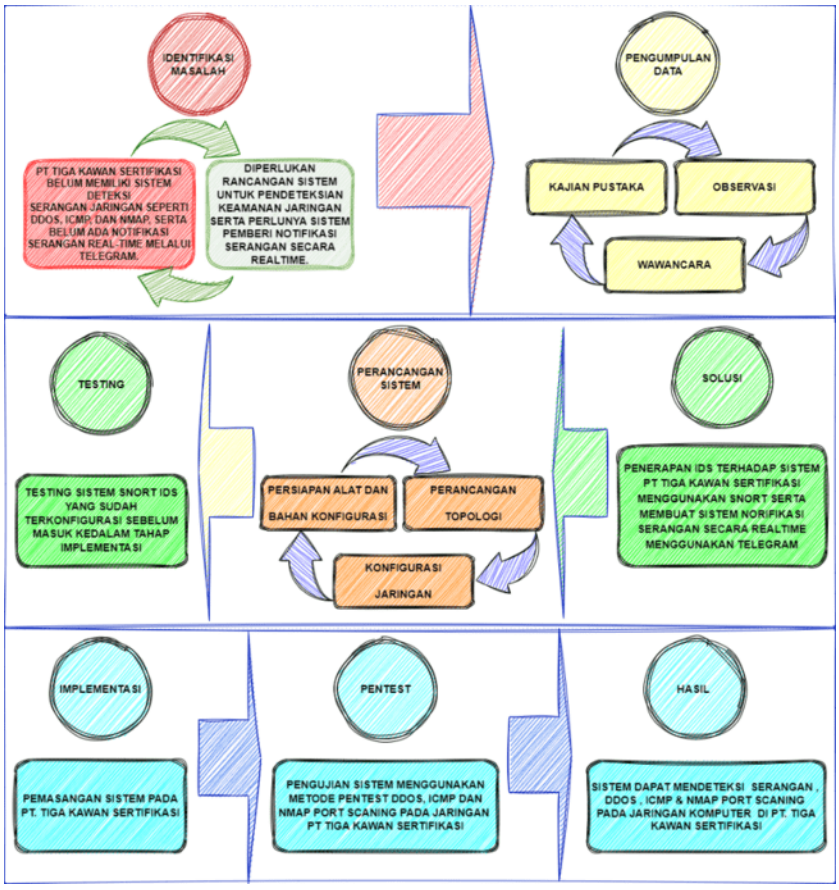
Dari ketiga penelitian tersebut, penulis menyimpulkan bahwa Snort dapat diandalkan sebagai sistem deteksi serangan pada jaringan. Namun, ada kekurangan dalam penelitian terdahulu, yaitu belum adanya sistem yang mengirim notifikasi serangan menggunakan aplikasi chat online yang user-friendly seperti WhatsApp atau Telegram. Aplikasi tersebut dapat membantu administrator jaringan memantau keamanan jaringan kapanpun dan dimanapun[18].

PT. Tiga Kawan Sertifikasi merupakan perusahan yang bergerak di bidang jasa legalitas atau perizinan yang berlokasi di Tangerang memiliki kendala pada saat ini dalam pengolaan system keamanan jaringan yang saat ini masih belum terkonfigurasi dengan baik, dimana dalam keamanan jaringan di perusahaan tersebut belum adanya sisitem deteksi serangan pada jaringan khususnya pada serangan DDOS , ICMP POD , NMAP Scaning serta memberi notifikasi serangan secara langsung kepada administrator jaringan.

Dari latar belakang tersebut penulis mendapatkan kesempatan untuk melakukan penelitian terhadap subjek yang dimana untuk mengidentifikasi dan mendeteksi serangan pada jaringan menggunakan SNORT serta menghubungkan Telegram sebagai media notifikasi alert untuk administrator jaringan

2. METODOLOGI PENELITIAN

Dalam penelitian ini penulis melibatkan penerapan metode Snort untuk membangun system deteksi serangan di PT. Tiga Kawan Sertifikasi dan melakukan metode pentest terhadap jaringan computer PT. Tiga Kawan Sertifikasi. Metodologi yang digunakan mencakup langkah-langkah dalam proses penelitian dapat dilihat pada gambar 2 Metodologi penelitian.



Gambar 2. Metodologi Penelitian

2.1. Metode Pengumpulan Data

Dalam penelitian ini penulis melakukan pengambilan data secara kualitatif, Teknik pada jaringan komputer menggunakan Snort. Menggunakan referensi dari penelitian sebelumnya juga memungkinkan penulis untuk mengevaluasi metodologi yang telah digunakan, memperoleh wawasan tentang tantangan yang mungkin dihadapi, serta menemukan peluang untuk pengembangan penelitian lebih lanjut. Dengan memanfaatkan wawasan dari berbagai sumber, penelitian ini bertujuan memberikan kontribusi berharga dalam pengembangan solusi sistem deteksi yang efektif dan efisien untuk keamanan jaringan komputer. pengambilan data kualitatif menggunakan 2 teknik yaitu pengambilan data primer dan skunder yang meliputi sebagai berikut:

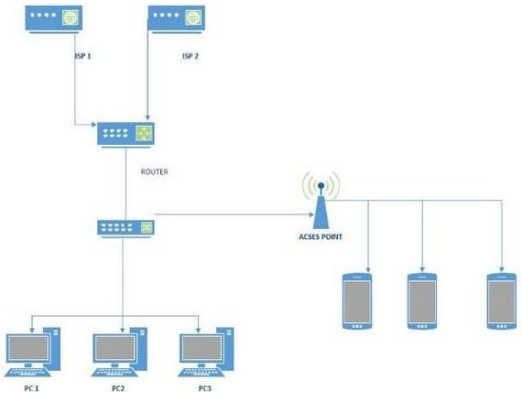
1. Data Primer
   a. Observasi: Dalam studi ini, penulis melakukan observasi langsung terhadap data perangkat jaringan serta struktur dan topologi jaringan di PT. Tiga Kawan Sertifikasi. Observasi ini meliputi pemeriksaan rinci terhadap jenis dan spesifikasi perangkat jaringan yang digunakan, seperti router, switch, dan perangkat endpoint lainnya, serta analisis terhadap konfigurasi topologi jaringan yang menunjukkan bagaimana perangkat-perangkat tersebut terhubung dan berinteraksi satu sama lain. Tujuan dari observasi langsung ini adalah untuk mendapatkan pemahaman yang mendalam mengenai kondisi jaringan saat ini dan kebutuhan spesifik perusahaan.

   b. Wawancara: Penulis melakukan wawancara langsung dengan staf IT PT. Tiga Kawan Sertifikasi sebagai bagian dari metodologi penelitian. Wawancara ini bertujuan untuk mendapatkan pemahaman mendalam tentang kebutuhan, preferensi, dan harapan tim IT terkait sistem yang akan dikembangkan. Selama wawancara, penulis berusaha menyampaikan informasi yang komprehensif mengenai rencana sistem yang sedang dirancang, serta mendengarkan dengan cermat tanggapan dan pertanyaan dari staf IT. Hal ini bertujuan memastikan bahwa sistem yang akan dibangun dapat memenuhi kebutuhan operasional perusahaan dan sesuai dengan harapan semua pihak yang terlibat.

2. Data Skunder
   Untuk mendukung penelitian ini, penulis merujuk pada 20 jurnal penelitian sebelumnya yang berfokus pada Snort, IDS, dan Keamanan Jaringan. Referensi-referensi ini menjadi dasar penting dalam pengumpulan data dan pemahaman mendalam mengenai konsep-konsep kunci yang berkaitan dengan topik penelitian. Melalui analisis jurnal-jurnal tersebut, penulis dapat mengidentifikasi tren, praktik terbaik, dan penemuan penting yang relevan untuk memandu proses perancangan dan implementasi sistem deteksi serangan.

2.2. Topologi

Topologi jaringan komputer adalah metode atau cara yang digunakan agar bisa menghubungkan satu komputer dengan komputer lainnya. Struktur atau jaringan yang digunakan untuk menghubungkan satu komputer dengan komputer lainnya bisa dengan menggunakan kabel atau pun nirkabel (tanpa kabel) [19], Dalam proses Pengumpulan data peneliti berhasil menghasilkan data, data yang dihasilkan dalam Pengumpulan data primer menggunakan observasi peneliti mendapatkan rancangan topologi pada PT. Tiga Kawan Sertifikasi , gambaran topologi tersebut berguna untuk peneliti melakukan perancangan system yang akan di implementasikan gambaran topologi tersebut dapat dilihat pada gambar 3.



Gambar 3 Topologi Eksisting

2.3. Alat Penelitian

Penelitian ini dilakukan menggunakan dua komponen yaitu perangkat lunak (software) dan perangkat keras (hardware).

1. Spesifikasi Perangkat Lunak (Software)
   Spesifikasi perangkat lunak adalah software yang digunakan sebagai penghubung dalam melakukan penelitian ini. Software yang di gunakan dapat dilihat pada table 1.

Tabel 1. Software

Perangkat Lunak	Detail Software	Deskripsi
Sistem Operasi IDS	Ubuntu 18	Sistem operasi ubuntu dipilih untuk di guna kanpada sistem IDS
Virtual Machine (VM)	Virtual Box	VirtualBox digunakan untuk membuat vm dalam penelitian ini dimana vm tersebut berisikan VM IDS & VM Attacker

Perangkat Lunak	Detail Software	Deskripsi
Sistem Operasi Attacker	Kali Linux	Dalam penggunaan sistem operasi untuk attacker peneliti mengguankan kali linux sebagai pentest dalam penelitian ini
Intrusion Detection System (IDS)	Snort	Untuk Sistem IDS yang digunakan dalam penelitian ini menggunakan SNORT yang dikonfigurasi dengan 3 rules yang digunakan dalam penelitian ini
Notifikasi	Telegram	Telegram berguna sebagai media notifikasi serangan pada jaringan snort.

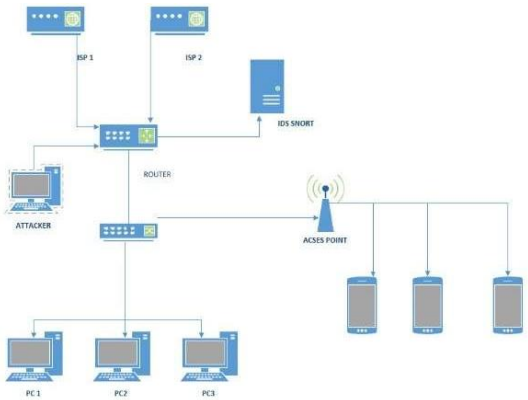
1. Spesifikasi Prangkat Keras (Hardware)
   Spesifikasi perangkat keras adalah perlatan yang digunakan sebagai pendukung dalam melakukan penelitian ini. Table 2 merupakan perangkat keras yang digunakan dalam melakukan penelitian ini.

Tabel 2. Hardware

Perangkat Keras	Detail Perangkat	Deskripsi
Laptop	Zyrex Cruiser 20 15v	Laptop berfungsi sebagai perangkat keras yang membantu penulis dalam melakukan konfigurasi sistem
Kabel Lan	RJ45	Kabel lan berfungsi untuk menghubungkan laptop ke mikrotik untuk masuk kedalam jaringan PT. TIga Kawan Sertifikasi

2.4. Rancangan Pengujian

Dalam penelitian ini, penulis telah merancang dengan cermat pengujian untuk sistem yang akan dikembangkan. Proses perancangan pengujian ini melibatkan penggunaan server ubuntu yang di konfigurasikan sebagai IDS menggunakan Snort [20] serta di konfigurasikan menggunakan chatbot telegram sebagai media pemberitahuan serangan secara realtime pada jaringan komputer , yang kemudian akan di hubungkan pada jaringan komputer PT. Tiga Kawan Sertifikasi serta penulis membuat satu server menggunakan Kali Linux sebagai server pentest untuk menguji sistem berikut gambaran topologi dari perancangan sistem dapat dilihat pada gambar 4.



Gambar 4. Rancangan Topologi

Serta dalam penelitian ini peneliti juga menetapakan ekspektasi dari rancangan pengujian yang sudah dibuat dalam tabel ekspektasi uat dalam serangan maupun deteksi, rancangan pengujian tersebut dapat di lihat pada tabel 3 UAT Pentest dan 4 UAT IDS SNORT.

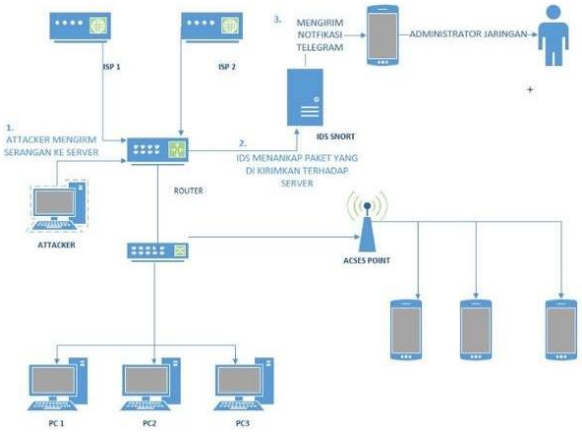
Tabel 3. UAT PENTEST

No	Pengujian	Ekspektasi
1	Penyerangan terhadap jaringan komputer menggunakan *Ping of death*	Berhasil
2	Penyerangan terhadap jaringan komputer menggunakan Nmap *port scaning*	Berhasil
3	Penyerangan terhadap jaringan komputer menggunakan DDoS	Berhasil

Tabel 4. UAT IDS SNORT

No	Pengujian	Ekspektasi
1	Pendeteksian serangan *Ping of death*	Berhasil
2	Pendektesian serangan Nmap *port scaning*	Berhasil
3	Pendektesian serangan DDoS	Berhasil

Alur kerja perancangan sistem dapat dilihat pada gambar dibawah ini pada Gambar 5 Rancangan alur pengujian sistem .



Gambar 5. Rancangan Alur pengujian system

3. HASIL DAN PEMBAHASAN

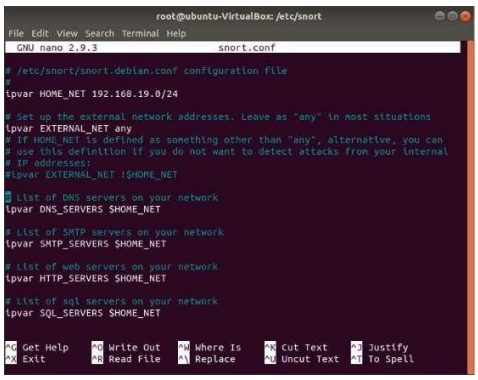
3.1. Implementasi

Implementasi adalah tindakan atau pelaksanaan dari sebuah rencana yang telah disusun dengan matang dan rinci. Biasanya, implementasi dilakukan setelah perencanaan dianggap sempurna[21], Dalam tahapan implementasi penulis melakukan konfigurasi terlebih dahulu terhadap sistem snort yang sebelumnya sudah di lakukan testing, dalam pengkonfigurasian sistem tersebut peneliti melakukan konfigurasi ip address pada server ids snort dan kali linux untuk attacker atau pentest seperti skema pengujian yang sudah dibahas pada sub bab 2.4 Rancangan Pengujian, berikut adalah data konfigurasi IP address dapat dilihat pada tabel 5.

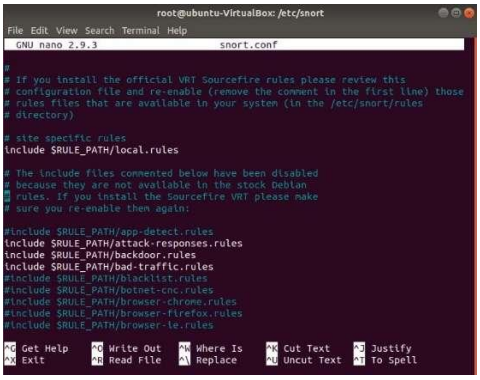
Tabel 5. Konfigurasi IP Address

Ip address kali linux (attacker)	Ip address ids snort
192.168.19.16	192.168.19.20

Dalam implementasi snort dibutuhkan penginstalan paket snort terlebih dahulu pada server ubuntu, lalu ada beberapa hal yang perlu dilakukan dalam pendeteksian snort agar dapat berjalan sesuai dengan yang diharapkan diantara nya dengan melakukan pembuatan rules snort terkait adanya ancaman supaya dapat terdekteksi oleh snort. Selanjutnya konfigurasi snort supaya snort dapat bekerja sebagai IDS untuk mendeteksi serangan[22]. Dalam konfigurasi snort ada hal yang penting perlu untuk dilaksanakan seperti untuk memasukan ip address client yang ingin dilindungin pada folder snort.conf dan snort.debian.conf, sehingga snort dapat berjalan mendeteksi jika adanya percobaan penyerangan terhadap ip client tersebut. Untuk lebih jelasnya dapat dilihat pada Gambar 6 Konfigurasi IP Snort.conf.



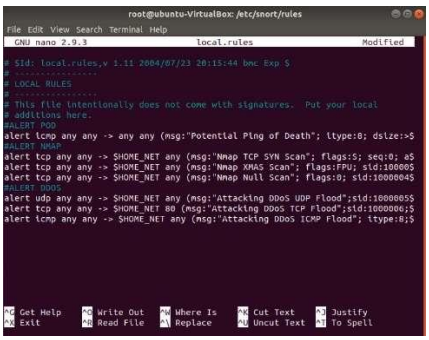
Gambar 6. Konfigurasi IP Snort.Conf



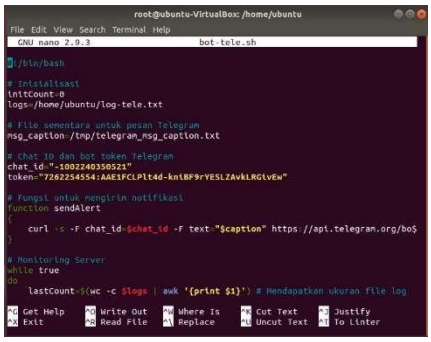
Gambar 7. Konfigurasi Dir Rules

Pada gambar 6 diatas dapat dilihat ip address yang ingin dilindungi oleh snort yang dimana ip nya 192.168.19.0/24. Selanjutnya memilih rules-rules snort yang dingin diaktifkan dengan menambahkan directori dari file rules yang sudah di buat di sini sya menaruh rules pada directori $RULE_PATH/local.rules. Setelah melakukan konfigurasi pada file `snort.conf`, langkah berikutnya adalah membuat aturan (rules) untuk Snort agar dapat mendeteksi serangan sesuai dengan jenis serangan yang diantisipasi dan konfigurasikan Snort dan

Telegram agar Snort dapat mendeteksi serangan dan mengirimkan peringatan kepada administrator atau pegawai IT melalui Telegram. Untuk lebih jelasnya dapat dilihat pada Gambar 8 dan Gambar 9.



Gambar 8. Konfigurasi Rules



Gambar 9. Konfigurasi Snort ke Telegram

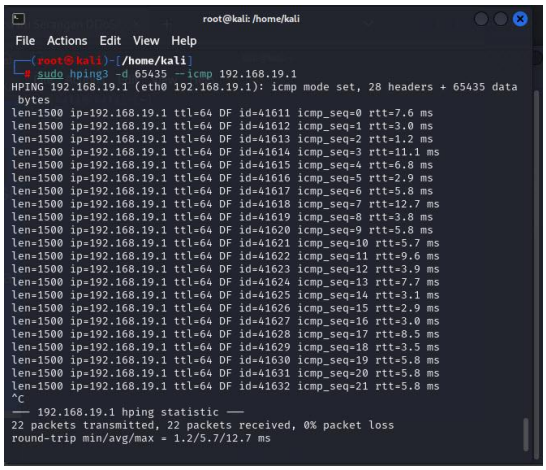
Untuk menjalakan snort kita harus masuk kedalam folder directory snort yaitu dengan cara **cd /etc/snort** dan setelah masuk kita dapat menuliskan perintah **snort -i enp0s3 -c /etc/snort/snort.conf -l /var/log/snort -d -A console > /home/server/log-tele.txt** untuk menjalankan snort dan kita juga perlu menjalankan bash telegram dimana dalam melakukan perintah bash telegram kita menggunakan perintah **./bot-tele.sh**

3.2. Pengujian Sistem (Pentest)

Dalam tahapan pengujian Komputer yang sudah terpasang snort akan mencoba mendeteksi adanya serangan atau aktivitas yang tidak wajar didalam jaringan yang terhubung ke server, dalam pengujian ini penulis melakukan penetrasi terhadap sistem menggunakan 3 metode serangan yaitu: POD (Ping off death), DDOS & NMAP Port Scannig.

3.2.1 *Ping Of Death*

Dalam pengujian ini penulis melakukan pentest dengan metode Ping Of Death menggunakan kali linux dengan perintah **sudo hping3 -d 654325 –icmp 192.168.19.1** dari serangan tersebut snort berhasil mendeteksi serangan Ping Of Death dan mengirimkan alert ke group telegram.

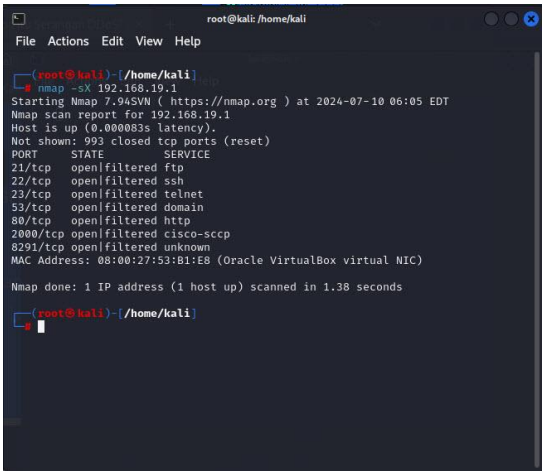


Gambar 10. Serangan Pod

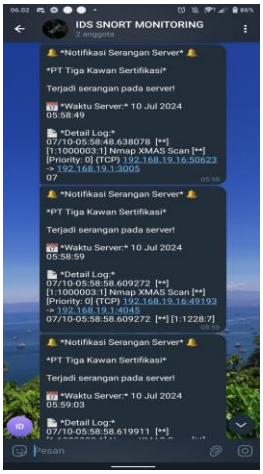
Gambar 11. Snort Alert Pod

3.2.2 Nmap *Port Scanning*

Lalu dalam pengujian selanjutnya penulis melakukan pengujian menggunakan Nmap Port scanning pengujian ini bertujuan untuk melihat port apa saja yang statusnya open atau terbuka pada jaringan PT. Tiga Kawan Sertifikasi, dalam pengujian tersebut snort berhasil mendeteksi serangan Nmap dan mengirimkan alert ke telegram pengujian tersebut dapat dilihat pada gambar gamabar 12 dan 13.



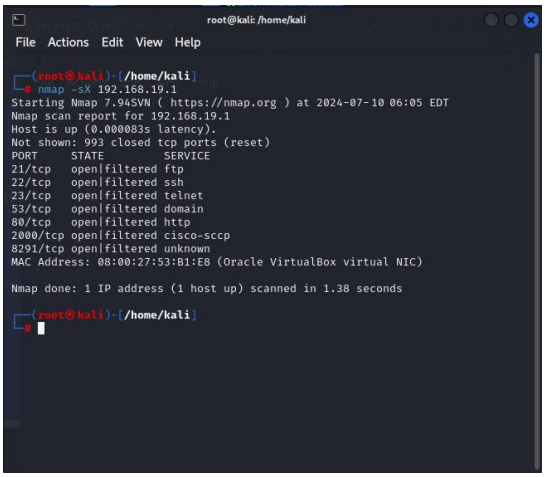
Gambar 12. Serangan Nmap



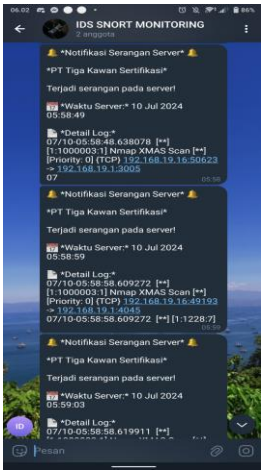
Gambar 13. Snort Alert Nmap

3.2.3 DDoS

Dan pada pengujian terakhir menggunakan serangan DDoS dengan metode UDP Flood menggunakan tools Hping 3 dengan menyerangan port 80 yang open berdasarakan informasi sebelumnya dari scnaing nmap, dalam penyerangan DDoS ini snort berhasil mendeteksi serangan dan mengirimkan alert ke telegram pengujian tersebut dapat dilihat pada gambar gambar 14 dan 15.



Gambar 14. Serangan DDoS



Gambar 15. Snort Alert DdoS

3.3. Hasil Akhir Pengujian

Hasil dari metode penetration test secara keseluruhan untuk pengujian keamanan Jaringan Komputer di PT. Tiga Kawan Sertifikasi pada tanggal 10 Juli 2024 dapat dilihat pada tabel di bawah ini. Pengujian ini mencakup berbagai jenis serangan untuk mengukur efektivitas sistem deteksi intrusi (IDS) Snort dalam mendeteksi dan merespon ancaman yang berpotensi membahayakan keamanan jaringan.

Tabel 6. waktu pengujian

No	Jenis serangan	Waktu		
		Awal serangan	Waktu Terdeteksi	Terkirim
1.	*Ping Of Death*	05:50:55	05:50:59	05:51:00
2.	Nmap *port scanning*	05:58:45	05:58:48	05:58:49
3.	DDoS UDP Hping3	06:04:58	06:05:00	06:05:00

Pengujian dilakukan dengan tiga jenis serangan berbeda, yaitu Ping of Death, Nmap port scanning, dan DDoS attack menggunakan Hping3. Waktu awal serangan dicatat, dan waktu ketika Snort berhasil mendeteksi serangan tersebut juga dicatat. Selain itu, waktu ketika peringatan dikirimkan kepada administrator juga diukur untuk mengevaluasi kecepatan respons sistem.

Tabel 7. Hasil Pengujian

No	Jenis serangan	Hasil pengujian sistem	Kesimpulan
1.	*Ping Of Death*	Terdeteksi	Berhasil
2.	Nmap *Port Scanning*	Terdeteksi	Berhasil
3.	DDoS UDP Hping3	terdeteksi	Berhasil

Dari tabel di atas, dapat dilihat bahwa seluruh pengujian mendapatkan hasil yang sesuai dengan yang diharapkan. Sistem Snort berhasil mendeteksi setiap jenis serangan yang dilakukan oleh attacker dengan tepat waktu. Pendeteksian serangan meliputi:

1. Ping of Death: Snort berhasil mendeteksi serangan ini dalam waktu 4 detik setelah serangan dimulai. Hal ini menunjukkan kemampuan sistem untuk mengenali paket ICMP besar yang berpotensi merusak.
2. Port Scanning (Nmap): Snort mendeteksi aktivitas port scanning dalam waktu 3 detik setelah serangan dimulai. Ini menunjukkan bahwa sistem dapat mengidentifikasi pola scanning yang sering digunakan oleh attacker untuk mencari celah keamanan.
3. DDoS Attack menggunakan Hping3: Snort mendeteksi serangan DDoS ini dalam waktu 2 detik setelah serangan dimulai, Ini menunjukkan kemampuan sistem dalam mengidentifikasi lalu lintas jaringan yang mencurigakan dan berpotensi membanjiri target.

Pendeteksian serangan sesuai dengan skenario yang dibuat, mulai dari Ping of Death, Nmap port scanning, hingga DDoS attack. Semua serangan terdeteksi dengan tepat waktu, menunjukkan bahwa sistem keamanan yang telah diterapkan mampu bekerja dengan efektif dan efisien dalam melindungi jaringan dari berbagai jenis ancaman. Keberhasilan dalam mendeteksi serangan ini menunjukkan bahwa konfigurasi Snort dan aturan yang diterapkan sudah optimal untuk mengamankan jaringan PT. Tiga Kawan Sertifikasi dari potensi serangan cyber.

4. KESIMPULAN

Berdasarkan hasil pengujian keamanan jaringan komputer di PT. Tiga Kawan Sertifikasi yang dipaparkan pada sub bab 3.2 Rancangan Pengujiann, penulis menarik kesimpulan sebagai berikut:

1. Sistem deteksi Snort yang digunakan sebagai IDS berhasil mendeteksi serangan Ping of Death, Nmap port scanning, dan DDoS sesuai dengan aturan (rules) yang telah dibuat. Sistem mampu mengklasifikasikan serangan berdasarkan aturan tersebut.
2. Berdasarkan waktu pengujian, Snort berhasil mendeteksi serangan jaringan yang dikirimkan sesuai dengan skenario pengujian. Serangan-serangan tersebut, yaitu Ping of Death, Nmap port scanning, dan DDoS dengan metode UDP, terdeteksi dalam waktu kurang dari 10 detik. Selain itu, Snort juga berhasil mengirimkan alert pada grup Telegram sebagai informasi serangan untuk administrator jaringan.
3. Metode Intrusion Detection System (IDS) Snort yang digabungkan dengan Telegram sebagai media notifikasi merupakan metode yang dapat mengoptimalkan tingkat keamanan jaringan komputer melalui pendeteksian serangan dan pemberitahuan serangan secara real-time. Dengan demikian, administrator dapat mengetahui serangan yang ada pada jaringan secara real-time dan dapat mengambil tindakan pencegahan dengan segera.

Penelitian ini diharapakan dapat ditingkatkan lagi, bukan hanya dalam skala jaringan LAN, tetapi juga pada skala jaringan MAN dan WAN. Selain itu, penelitian ini perlu terus dikembangkan, mulai dari aturan (rules) Snort itu sendiri hingga kemampuan untuk memperbarui rules secara otomatis dan meningkatkan mekanisme respon otomatis. Diharapkan juga penelitian ini dapat dikembangkan agar sistem IDS ini dapat secara otomatis memblokir serangan dan mengirimkan peringatan ke aplikasi Telegram tanpa perlu mengaktifkan Snort di Linux Ubuntu terlebih dahulu. Dengan demikian, sistem ini akan lebih efektif dan efisien dalam memberikan perlindungan jaringan serta mempermudah administrator jaringan dalam memantau dan menangani serangan secara real-time.

REFERENSI

[1] APJII, “APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang,” APJII. Accessed: May 19, 2024. [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20mengumumkan%20jumlah%20pengguna%20internet,jiwa%20penduduk%20Indonesia%20tahun%202023.

[2] D. I. Mulyana, F. Ardiyansyah, N. Hidayat, and A. Zulfikar, “Optimasi Keamanan Jaringan Wifi dari Situs Judi Online dan Pornografi dengan DNS Filtering dan Orangepi,” *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 2, pp. 647–655, Mar. 2024, doi: 10.57152/malcom.v4i2.1274.

[3] C. A. Putra *et al.*, *DETEKSI SERANGAN TROJAN HORSE DENGAN MEMANFAATKAN IDS SNORT*. 2019.
[4] I. Gede, W. Bangga, and S. M. Ladjamuddin, "SIMULASI SNORT SEBAGAI ALAT PENDETEKSI INTRUSI PADA WEB DAMN VULNERABLE WEB APPLICATION," *Jurnal Rekayasa Informasi*, vol. 11, no. 2, 2022.
[5] Biro Hukum dan Komunikasi Publik – BSSN, "BSSN Ungkap Lanskap Keamanan Siber Indonesia Tahun 2022 untuk Literasi Budaya Keamanan Siber," BADAN SIBER DAN SANDI NEGARA. Accessed: Jul. 17, 2024. [Online]. Available: https://www.bssn.go.id/lanskap2022/
[6] J. Khatib Sulaiman, A. Nugraha, D. Aulia Gustian, and U. Dian Nuswantoro Semarang, "Deteksi Malware Dridex Menggunakan Signature-based Snort," *Indonesian Journal of Computer Science Attribution-ShareAlike*, vol. 4, no. 1, p. 54, 2021.
[7] Putra Ansa Gaora, "Kepemimpinan Digital dan Masa Depan Keamanan Siber Kita," DetikNews. Accessed: Jun. 13, 2024. [Online]. Available: https://news.detik.com/kolom/d-7146308/kepemimpinan-digital-dan-masa-depan-keamanan-siber-kita
[8] A. G. Gani, "KONFIGURASI SISTEM KEAMANAN JARINGAN."
[9] R. Fauzi, Y. Muhyidin, and D. Singasatia, "Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS)," 2023.
[10] A. Ekawijana, A. Bakhrun, and T. Kurniawan, "JURNAL MEDIA INFORMATIKA BUDIDARMA Deteksi Serangan DDOS Pada Jaringan SDN dengan Metode Random Forest," 2024, doi: 10.30865/mib.v8i1.6928.
[11] CyberSecurity, "Jenis-Jenis Serangan Siber di Era Digital," BPPTIK KOMINFO. Accessed: Jun. 13, 2024. [Online]. Available: https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital
[12] Suhartono, "SISTEM PENGAMANAN JARINGAN ADMIN SERVER DENGAN METODE INTRUSION DETECTION SYSTEM (IDS) SNORT MENGGUNAKAN SISTEM OPERASI CLEAROS," 2017.
[13] M. Pitriyanti, N. Khairani Daulay, and M. Agus Syamsul Arifin, "KLIK: Kajian Ilmiah Informatika dan Komputer Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort," *Media Online*, vol. 3, no. 4, pp. 323–329, 2023, [Online]. Available: https://djournals.com/klik
[14] I. Putu, A. E. Pratama, N. Kade, and M. Handayani, "IMPLEMENTASI IDS MENGGUNAKAN SNORT PADA SISTEM OPERASI UBUNTU," *Jurnal Mantik Penusa*, vol. 3, no. 1, pp. 176–181, 2019, [Online]. Available: www.snort.org
[15] T. Aprilianto, S. Jatmika, and I. Wicaksono, "PERANCANGAN SISTEM PENDETKSI SERANGAN PADA SERVER JARINGAN KOMPUTER MENGGUNAKAN SNORT BERBASIS SMS GETEWAY," vol. 11, no. 1, p. 4345225.
[16] Z. Dwi Alfaeni, N. Fahriani, J. Raya Sutorejo No, D. Sutorejo, K. Mulyorejo, and J. Timur, "Zulhelmi Dwi Alfaeni, Deteksi Serangan Ddos Pada Jaringan Rt/Rw-Net Desa Ketanen Dengan Metode Intrusion Detection System (IDS) Menggunakan Snort Deteksi Serangan Ddos Pada Jaringan Rt/Rw-Net Desa Ketanen Dengan Metode Intrusion Detection System (IDS) Menggunakan Snort".
[17] "Rancang Bangun Aplikasi Deteksi dan Penanganan Serangan DDOS dan Port Scanning Memanfaatkan SNORT Pada Jaringan Komputer".
[18] "IMPLEMENTASI HONEYPOT COWRIE DAN SNORT SEBAGAI ALAT DETEKSI SERANGAN PADA SERVER".
[19] Administrator, "Kenali Apa Itu Topologi Jaringan dan Apa Saja Jenisnya. Ayo Simak Lebih Lanjut," DISKOMINFO. Accessed: May 21, 2024. [Online]. Available: https://diskominfo.kuburayakab.go.id/read/4/kenali-apa-itu-topologi-jaringan-dan-apa-saja-jenisnya-ayo-simak-lebih-lanjut
[20] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 4, no. 2, p. 413, Apr. 2020, doi: 10.30865/mib.v4i2.2037.
[21] Anindyadevi Aurellia, "Apa Itu Implementasi? Pengertian, Tujuan, dan Contoh Penerapannya," DetikNews. Accessed: May 21, 2024. [Online]. Available: https://www.detik.com/jabar/berita/d-6185222/apa-itu-implementasi-pengertian-tujuan-dan-contoh-penerapannya
[22] H. Yanto, "Intruder Detection Monitoring System in Computer Networks Using Snort Based Sms Alert (Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Berbasis Sms Alert)," *Jurnal KomtekInfo*, vol. 7, no. 2, 2020, doi: 10.35134/komtekinfo.v7i2.