Jurnal Ilmu Komputer Revolusioner

Vol.9 No.6, Juni 2025
ISSN: 24430355

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT SEBAGAI SISTEM KEAMANAN MENGGUNAKAN WHATSAPP DAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI DI KANTOR CAMAT WARA KOTA PALOPO

Rasni. S Tandi. A[1], Siaulhak[2], Jumarniati[3]
Universitas Cokroaminoto Palopo
E-mail: rasnirasni69@gmail.com[1], siaulhak@uncp.ac.id[2], jumarniati@uncp.ac.id[3]

Abstrak

Tujuan dari penelitian ini adalah mengimplementasikan Intrusion Detection System (IDS) snort pada jaringan komputer di kantor camat wara kota palopo sebagai upaya pengamanan dan mengimplementasikan whatsapp dan telegram sebagai media notifikasi untuk memberi informasi ancaman kepada administrator jaringan. Jenis penelitian yang digunakan yaitu penelitian research and development (R&D) yang sudah di kembangkan berdasarkan kebutuhan. Sedangkan model atau tahapan penelitian yang digunakan dalam penelitian ini menggunakan model ndlc (network design life cycle) yaitu analisis (analysis), perancangan (design), simulasi (simulation prototyping), implementasi (implementation), monitoring, dan management, sehinggan rangkaian proses penelitian dapat di lakukan secara terarah, teratus dan sistematis. Berdasarkan hasil dari rangkaian hasil penelitian implementasi Intrusion Detection System (IDS) snort sebagai sistem keamanan menggunakan whatsapp dan telegram sebagai media notifikasi di kantor camat wara kota palopo terhadap rumusan dan batasan masalah yang ada, maka penulis dapat menyimpulkan bahwa, pengimplementasian snort IDS menggunakan OS ubuntu 2022 dengan menginstal IDS secara langsung dari repository snort kemudian melakukan pengaturan rules dan validasi snort pada OS ubuntu. Kemudian pengitegrasian whatsapp dan telegram sebagai penerima notifikasi snort IDS dilakukan membuat boot pada masing-masing aplikasi untuk menerima notifikasi secara realtime. Untuk boot whatsapp menggunakan aplikasi pihak ketiga yaitu twilio sedangkan telegram menggunakan boot father yang telah ada pada aplikasi telegram.
Kata Kunci — Intrusion Detection System; Sistem Keamanan; Whatsapp Dan Telegram.

Abstract

The purpose of this study is to implement the Snort Intrusion Detection System (IDS) on the computer network at the Wara sub-district office in Palopo City as a security effort and to implement WhatsApp and Telegram as notification media to provide threat information to network administrators. The type of research used is research and development (R&D) research that has been developed based on needs. While the model or stages of research used in this study use the ndlc (network design life cycle) model, namely analysis, design, simulation (simulation prototyping), implementation, monitoring, and management, so that the series of research processes can be carried out in a directed, orderly and systematic manner. Based on the results of a series of research results on the implementation of the Snort Intrusion Detection System (IDS) as a security system using WhatsApp and Telegram as notification media at the Wara sub-district office in Palopo City regarding the formulation and limitations of the existing problems, the author can conclude that the implementation of Snort IDS uses the Ubuntu 2022 OS by installing IDS directly from the Snort repository and then setting the rules and validating Snort on the Ubuntu OS. Then the integration of WhatsApp and Telegram as recipients of Snort IDS notifications is carried out by creating a boot on each application to receive notifications in real time. To boot WhatsApp, a third-party application is used, namely Twilio, while Telegram uses the Boot Father that is already in the Telegram application.
Keywords *— Intrusion Detection System; Security System; Whatsapp And Telegram.*

1. PENDAHULUAN

Seiring berkembangnya teknologi dan meningkatnya kemampuan individu dalam bidang peretasan (hacking), isu mengenai keamanan jaringan menjadi semakin krusial. Banyaknya aplikasi dan alat bantu yang tersedia memudahkan penyerang (attacker) dalam mengeksploitasi celah keamanan pada jaringan maupun server. Dalam konteks ini, sistem keamanan jaringan komputer memegang peran vital dalam menjaga keutuhan data (integritas), memastikan data hanya dapat diakses oleh pihak yang sah (validitas), serta menjamin layanan tetap tersedia bagi pengguna yang berwenang. Serangan siber bisa terjadi kapan pun, tidak mengenal waktu maupun kondisi, baik ketika administrator sedang aktif mengelola sistem maupun saat sistem berjalan otomatis. Oleh karena itu, diperlukan adanya mekanisme perlindungan internal yang mampu melakukan deteksi secara real-time. Peningkatan intensitas penggunaan internet juga turut memperbesar risiko serangan terhadap jaringan, sehingga pengawasan terhadap akses dan upaya pencegahan penggunaan ilegal terhadap sumber daya jaringan harus menjadi perhatian utama dalam sistem keamanan [1].

Penetration testing merupakan salah satu metode evaluasi keamanan yang bernilai strategis, baik dari sisi bisnis maupun operasional perusahaan. Dari perspektif operasional, metode ini berperan penting dalam merumuskan kebijakan dan strategi keamanan informasi dengan cara mendeteksi berbagai kerentanan secara cepat dan tepat. Web server sendiri memiliki fungsi utama untuk melayani permintaan protokol HTTP dari klien yang terhubung melalui jaringan, serta menyajikan informasi dalam bentuk halaman web yang dapat diakses melalui browser. Namun, dalam praktiknya, sering terjadi gangguan seperti server lambat merespons permintaan, sistem menjadi tidak stabil, atau bahkan tidak dapat diakses sama sekali. Gangguan semacam ini kerap kali disebabkan oleh kerusakan sistem akibat serangan dari pihak tidak bertanggung jawab (hacker). Maka dari itu, sangat penting dilakukan upaya identifikasi terhadap celah keamanan yang ada pada sistem web server agar potensi eksploitasi oleh penyerang dapat diminimalkan. Salah satu solusi efektif yang dapat diterapkan adalah dengan melakukan penetration testing secara berkala untuk mendeteksi kelemahan dan mencegah gangguan layanan yang bisa merugikan pengguna maupun pemilik sistem [2].

Selain melakukan pengujian penetrasi (penetration testing), penerapan Intrusion Detection System (IDS) juga menjadi langkah preventif yang sangat penting dalam menjaga keamanan infrastruktur jaringan. IDS merupakan mekanisme yang dirancang untuk mengidentifikasi potensi serangan atau upaya intrusi terhadap komputer maupun server yang terhubung dalam suatu jaringan. Sistem ini bekerja dengan cara memantau lalu lintas jaringan secara terus-menerus guna mendeteksi aktivitas mencurigakan yang berasal dari luar sistem, terutama serangan yang mencoba menembus jaringan internal melalui internet. Namun, IDS tidak hanya sekadar mendeteksi; sistem ini juga memerlukan proses lanjutan untuk mengklasifikasikan dan memberikan notifikasi terhadap jenis serangan berdasarkan pola karakteristik tertentu. Salah satu jenis IDS yang paling dikenal dan banyak digunakan dalam lingkungan profesional adalah Snort [3]. Snort merupakan perangkat lunak sumber terbuka yang mampu mengidentifikasi dan menganalisis aktivitas jaringan yang mencurigakan. Dengan kemampuan menangkap, mencatat, dan memeriksa paket data secara real-time, Snort dapat mendeteksi berbagai jenis ancaman eksternal. Program ini memiliki tiga mode utama, salah satunya adalah mode Packet Sniffer, yang memungkinkan pengguna untuk memantau lalu lintas data yang sedang berlangsung dalam jaringan secara langsung. Paket Logger, berfungsi untuk menyimpan seluruh paket yang lewat di jaringan untuk dianalisis di kemudian hari. Paket Network Intrusion Detection System NIDS, Snort berfungsi untuk mendeteksi serangan yang dilakukan melalui

jaringan komputer [4].

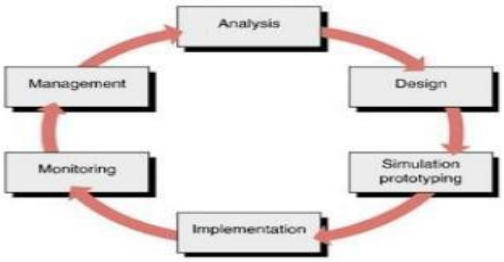
Hasil observasi di Kantor Camat Wara Kota Palopo menunjukkan bahwa Kantor Camat Wara Kota Palopo memiliki sejumlah masalah terkait dengan pengelolaan keamanan jaringan. Salah satu masalah utama yang dihadapi adalah kurangnya pemahaman yang mendalam tentang teknik pengujian penetrasi yang efektif. Hal ini menyebabkan jaringan komputer di Kantor Camat menjadi rentan terhadap gangguan dari luar, meskipun sudah ada pengaturan dasar mengenai pengamanan. Selain itu, Kantor Camat Wara Kota Palopo juga menghadapi masalah dalam implementasi sistem deteksi intrusi yang efektif. Meskipun ada beberapa upaya untuk mengintegrasikan sistem IDS, namun implementasinya belum optimal. Kurangnya pemahaman tentang cara mengonfigurasi dan memanfaatkan sistem IDS yang ada menghambat kemampuan sekolah untuk mendeteksi dan merespon ancaman secara cepat dan tepat.

Mengatasi permasalahan tersebut dapat dilakukan dengan penerapan IDS yang diharapkan mampu meningkatkan keamanan jaringan dari ancaman yang terus berkembang. Selain mendeteksi ancaman eksternal seperti serangan dari pihak ketiga, IDS juga memainkan peran penting dalam mengidentifikasi ancaman internal, misalnya aktivitas pengguna yang melanggar kebijakan keamanan atau perangkat yang terinfeksi malware. Hal ini sangat relevan di lingkungan pemerintahan seperti kantor camat, yang sering kali memiliki jaringan yang kompleks dan rentan terhadap serangan. Dengan mengintegrasikan Intrusion Detection System (IDS) ke dalam infrastruktur jaringan, kantor camat dapat meningkatkan kesiapsiagaan terhadap serangan siber, melindungi data penting, serta menciptakan lingkungan digital yang lebih aman bagi pegawai dan pelayanan masyarakat.

Berdasarkan uraian tersebut penulis akan melakukan penelitian yang berjudul “Implementasi Intrusion Detection System (IDS) Snort Sebagai Sistem Keamanan Menggunakan WhatsApp dan Telegram Sebagai Media Notifikasi di Kantor Camat Wara Kota Palopo”.

2. METODE

Penelitian ini menggunakan pendekatan metode Research and Development (R&D), yakni suatu metode yang bertujuan untuk mengembangkan serta menghasilkan produk tertentu, kemudian menguji tingkat efektivitas dari produk tersebut dalam konteks yang ditentukan. Dalam pelaksanaannya, penelitian ini mengadopsi model Network Development Life Cycle (NDLC), yang merupakan kerangka kerja sistematis dalam proses perancangan dan pengembangan jaringan komputer. NDLC memuat tahapan-tahapan penting yang menggambarkan siklus hidup pembangunan sistem jaringan secara terstruktur dan berkesinambungan, mulai dari perencanaan awal hingga pengelolaan sistem [5]. Istilah "Cycle" pada NDLC menekankan bahwa proses ini bersifat iteratif dan mencakup seluruh proses pembangunan jaringan secara menyeluruh. Secara umum, metodologi NDLC terdiri atas enam tahapan utama, yaitu Analysis, Design, Simulation Prototype, Implementation, Monitoring, dan Management. Namun, dalam penelitian ini, proses hanya difokuskan hingga tahap Implementasi, guna mengevaluasi efektivitas rancangan sistem jaringan yang dikembangkan. Adapun kerangka penelitian yang digunakan menggambarkan langkah-langkah penerapan NDLC secara sistematis sesuai kebutuhan studi ini.



Gambar 1. Metode NDLC

3. HASIL DAN PEMBAHASAN

Tahap hasil penelitian ini memaparkan penerapan Intrusion Detection System (IDS) Snort sebagai solusi keamanan jaringan yang telah diimplementasikan di Kantor Camat Wara Kota Palopo. Dalam sistem ini, WhatsApp dan Telegram digunakan sebagai media notifikasi untuk memberikan peringatan secara cepat dan efisien ketika terjadi aktivitas mencurigakan atau serangan pada jaringan. Melalui hasil implementasi tersebut, dapat dievaluasi sejauh mana sistem keamanan yang dikembangkan memenuhi standar keamanan yang dibutuhkan serta efektivitasnya dalam menjaga keamanan jaringan di lingkungan Kantor Camat Wara Kota Palopo. Metode yang digunakan dalam pengembangan jaringan ini adalah Network Development Life Cycle (NDLC), yaitu suatu kerangka kerja yang mendefinisikan tahapan proses perancangan dan pengembangan sistem jaringan komputer secara terstruktur. Metode NDLC terdiri dari beberapa fase utama, yaitu Analisis (Analysis), Perancangan (Design), Simulasi atau Prototipe (Simulation Prototyping), Implementasi (Implementation), Pemantauan (Monitoring), dan Manajemen (Management). Pendekatan ini membantu memastikan bahwa setiap langkah pengembangan sistem dilakukan secara sistematis dan berkelanjutan sehingga menghasilkan sistem yang handal dan sesuai kebutuhan

1. Analysis

a. Observasi

Hasil observasi di Kantor Camat Wara Kota Palopo menunjukkan bahwa Kantor Camat Wara Kota Palopo memiliki sejumlah masalah terkait dengan pengelolaan keamanan jaringan. Salah satu masalah utama yang dihadapi adalah kurangnya pemahaman yang mendalam tentang teknik pengujian penetrasi yang efektif. Hal ini menyebabkan jaringan komputer di Kantor Camat menjadi rentan terhadap gangguan dari luar, meskipun sudah ada pengaturan dasar mengenai pengamanan.

b. Wawancara

Pada tahap wawancara dilakukan dengan wawancara lagsung. Wawancara dilakukan dengan memberikan pertanyaan langsung kepada kepala sekolah sebagai bagian dari proses wawancara yang dilakukan.

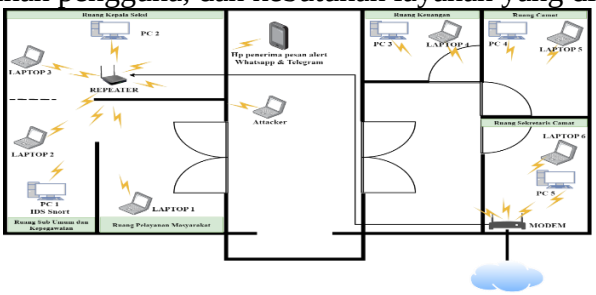
c. Studi pustaka

Hasil dari studi pustaka yang penulis lakukan untuk memperkuat penelitian ini adalah dengan mencari referensi mengenai konsep dan teknik dari buku, jurnal, maupun tugas akhir yang di mana terdapat dalam tinjauan pustaka dan landasan teori.

2. Design

Tahap perancangan ini penulis akan membuat gambar design topology jaringan interkoneksi yang akan dibangun, design bisa berupa design struktur topology, design akses data, design tata layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang network yang akan dibangun serta hasil analisis kebutuhan

perangkat, kebutuhan pengguna, dan kebutuhan layanan yang di perlukan.



Gambar 2. Topologi Sietem Keamanan Jaringan yang Dibangun

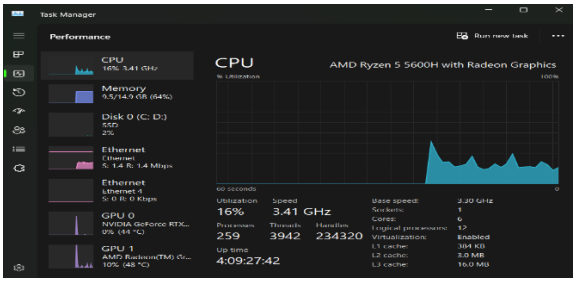
a. Analisis Kebutuhan Perangkat Keras (Hardware)
   1) Laptop Intel® Celeron® N4020 (2 core / 2 thread, 1.1 GHz hingga 2.8 GHz, cache 4MB)
   2) Perangkat input dan output.
   3) Modem
   4) Switch
b. Analisis Kebutuhan Perangkat Lunak (Software)
   1) Sistem Operasi Windows 10 64 bit.
   2) OS Ubuntu
   3) OS Kali Linux
   4) Virtual Box
   5) IDS Snort
   6) Whatsapp
   7) Bot Telegram
   8) Twilio

3. Simulation Prototyping

Dari arsitektur dan topologi yang sudah penulis peroleh, pada tahap ini penulis akan melakukan simulasi pengujian sistem. Pengujian ini dilakukan pada saat jaringan normal tanpa ada penerapan IDS snort.

Gambar 3. Penyerangan DDoS menggunakan Kali Linux

Berdasarkan gambar di atas penulis melakukan penyerangan pada jaringan LAN laboratorium komputer menggunakan OS Kali Linux. aplikasi yang digunakan untuk menyerang adalah hping 3 dengan mengetik perintah “hping3 -1 192.168.1.1 --flood” pada terminal.



Gambar 4. Tampilan Performa Jaringan Setelah di Lakukan Penyerangan

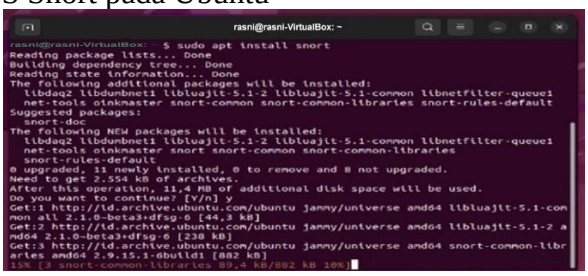
Berdasarkan gambar di atas setelah melakukan penyerangan DDoS penulis mengecek performa jaringan dan didapatkan bahwa konkesi jaringan meningkat sehingga

membuat pengguna jaringan lain terganngu sehingga koneksi internet tidak stabil.

4. Implementation

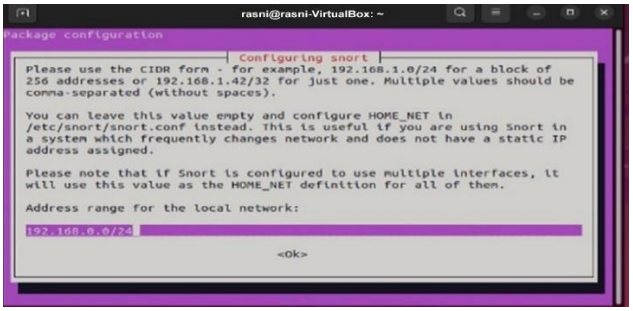
Dari hasil simulasi yang sudah penulis peroleh, pada tahap ini penulis akan melakukan implementasi intrusion detection system (IDS) snort sebagai sistem keamanan menggunakan whatsapp dan telegram sebagai media notifikasi di Kantor Camat Wara Kota Palopo. Pada tahap ini dilakukan penginstalan snort pada server ubuntu dan konfigurasi rules pada snort untuk mendeteksi penyerang.

a. Konfigurasi IDS Snort pada Ubuntu



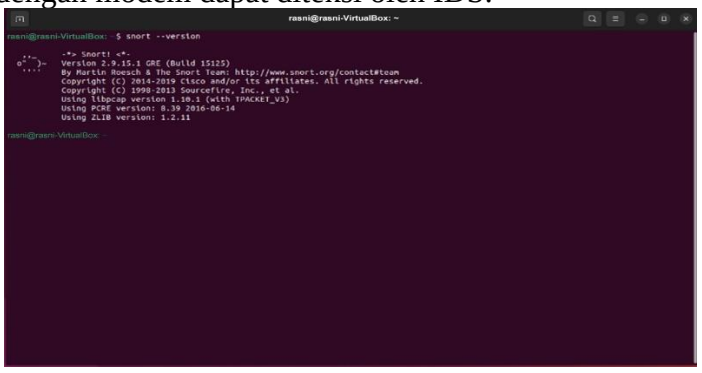
Gambar 5. Penginstalan IDS Snort

Pada langka awal peneliti menginstal snort pada ubuntu dengan perintah “sudo apt install snort” pada terminal.



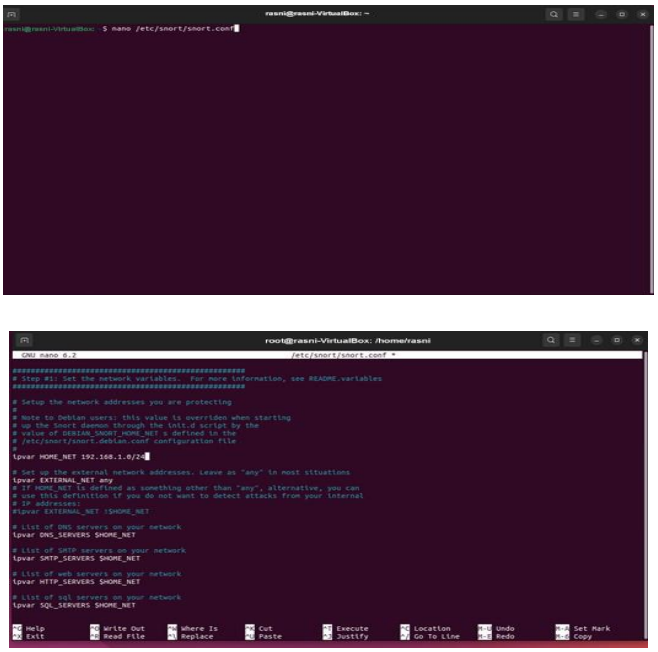
Gambar 6. Konfigurasi IP Address Server IPS

Berdasarkan gambar di atas penulis melakukan konfigurasi IP server IDS snort dengan mengisi IP address “192.168.1.0/24”. hal ini dilakukan agar semua IP address yang tersambung dengan modem dapat diteksi oleh IDS.



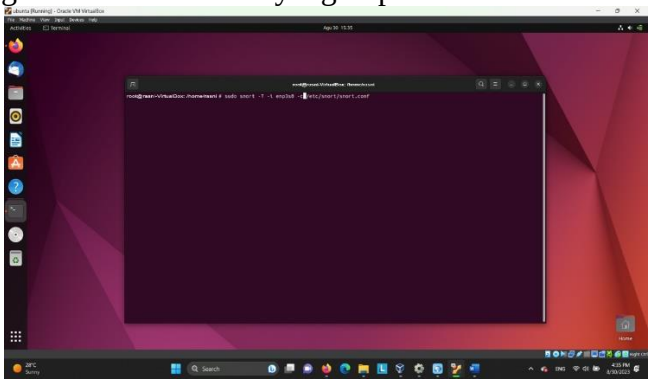
Gambar 7. Memeriksa Versi Snort

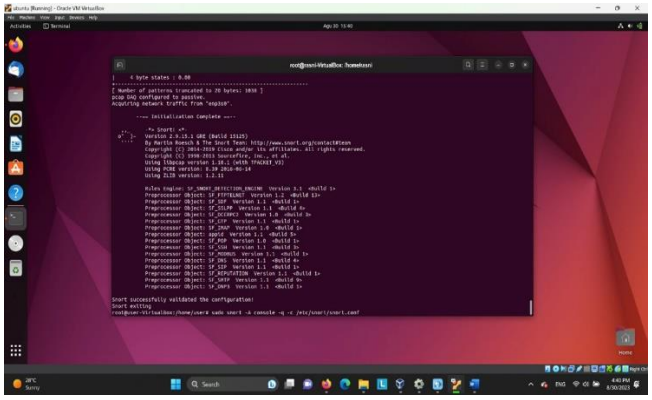
Berdasarkan gambar di atas penulis melakukan konfigurasi IP server IDS snort dengan mengisi IP address “192.168.1.0/24”. hal ini dilakukan agar semua IP address yang tersambung dengan modem dapat diteksi oleh IDS.



Gambar 8. Melakukan Konfigurasi Snort

Berdasarkan gambar di atas penulis melakukan konfigurasi Snort dengan perintah "sudo /etc/snort/snort.conf". Kemudian pada ipvar HOME_NET diberikan IP address 192.168.1.0/24 sebagai IP address utama yang di proteksi oleh IDS.



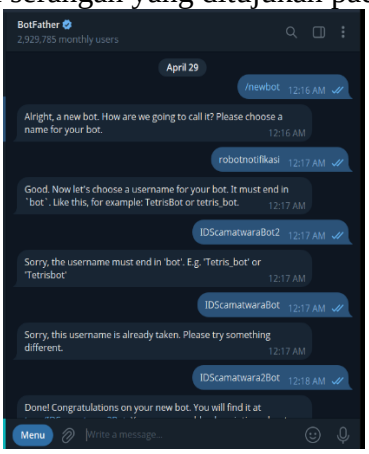


Gambar 9. Melakukan Validasi Rules Snort

Berdasarkan gambar di atas setelah melakukan konfigurasi snort penulis melanjutkan melakukan validasi rules dengan perintah "sudo snort -T -I enp3s0 -c /etc/snort/snort.conf".

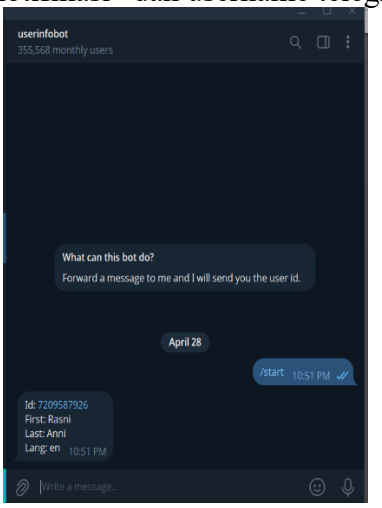
b. Konfigurasi Bot Telegram

Setelah IDS snort berhasil di konfigurasi dan berjalan dengan baik, langkah selanjutnya membuat bot telegram sebagai penerima alert (peringatan) apabila IDS snort mendeteksi adanya serangan yang ditujukan pada sistem keamanan jaringan.



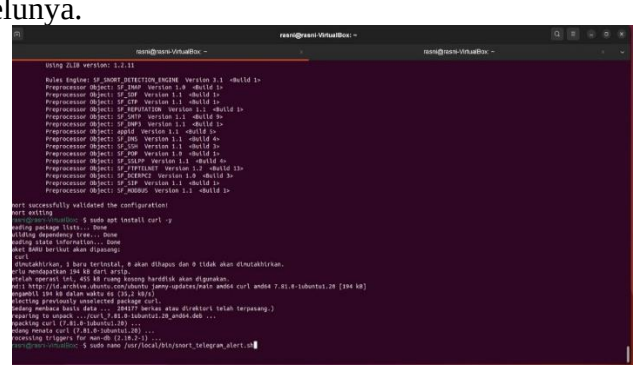
Gambar 10. Mebuat Bot Telegram

Bot telegram dibuat dengan mengakses BotFther pada telegram kemudian mengetik /newbot dan membuat notifikasi berdasarkan kebutuhan. Disini penulis membuat bot telegram dengan nama “robot notifikasi” dan username telegram “IDScamatwaraBot2”.



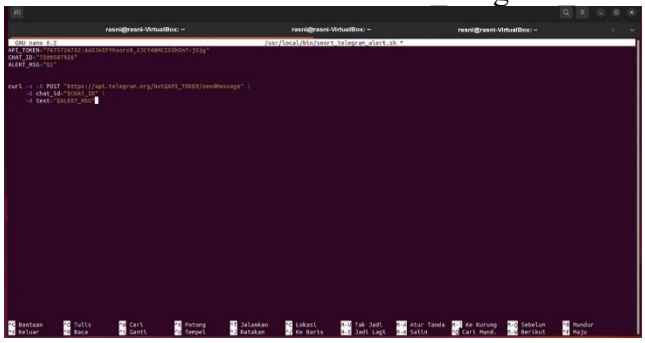
Gambar 11. Melihat ID User

Berdasarkan gambar di atas penulis mengakses “userinfobot’ untuk mendapatkan ID user dari bot telegram yang dibuat sebelumnya. Hal ini diperlukan dikarenakan untuk membuat IDS snort mengirimkan notifikasi harus menggunakan ID user dan IP token dari bot yang dibuat sebelunya.



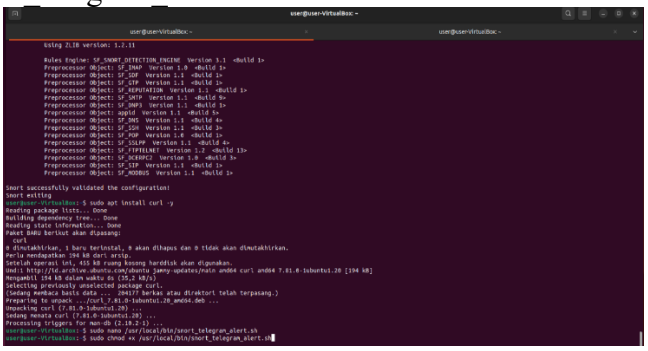
Gambar 12. Membuat Konfigurasi Notifikasi Telegram

Setelah pembuatan bot telegram selesai, penulis melakukan konfigurasi pada IDS snort agar notifikasi dapat terkirim ke bot telegram jika terjadi penyerangan pada sistem. Dengan cara mengetik “sudo nano /usr/local/bin/snort_telegram_alert.sh”.



Gambar 13. Membuat Skrip Notifikasi Telegram

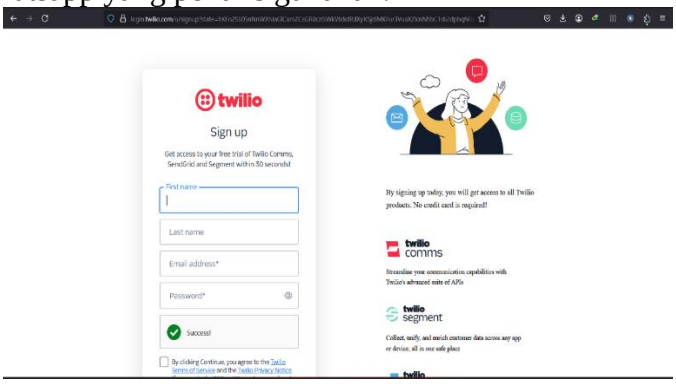
Gambar diatas merupakan skrip konfigurasi alert telegram untuk mengirimkan notifikasi pada bot telegram jika serangan terjadi. Setelah selesai dibuat penulis menyimpan skrip tersbut dengan menekan “CTRL X” kemudian enter. Kemudian memerikan akses agar IDS dapat mengakses skrip tersebut dengan perintah “sudo shmod +x /usr/local/bin/snort_telegram_alert.sh”.



Gambar 14. Memberikan Ijin Akses pada Snort

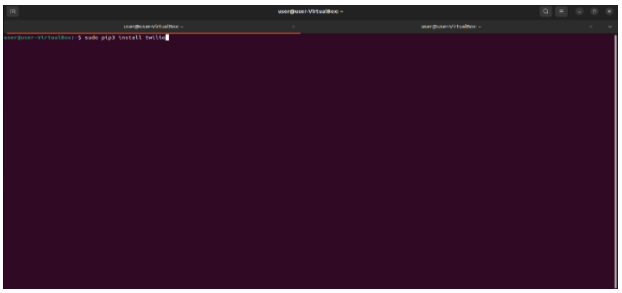
c. Konfigurasi Whatsapp

Pada konfigurasi ini aplikasi whatsapp tidak menyediakan jasa bot pada aplikasinya melainkan harus menggunakan pihak ke tiga untuk membuat bot pada aplikasi ini. Disini penulis menggunkan twilio untuk membuat bot dan dihubungkan pada nomor whatsapp yang penulis gunakan.



Gambar 15. Form Pendaftaran Twilio

Berdasarkan gambar di bawah penulis melakukan instalasi twilio pada ubuntu agar dapat digunakan oleh IDS snort dengan perintah “sudo apt install twilio -y”.

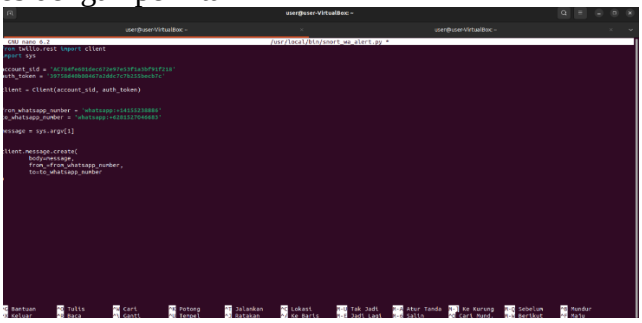


Gambar 16. Pengistalan Twilio pada Ubuntu

Setelah penginstalan twilio penulis membuat skrip pada IDS snort agar dapat mengirimkan notifikasi whatsapp melalui twilio. Pada skrip ini penulis menggunakan python 3 dikarenakan twilio hanya mengenali skrip tersebut dengan cara mengetik “sudo nano /usr/local/bin/snort_wa_alert.py”. untuk skrip dapat di lihat pada gambar di bawah ini.

Gambar 17. Pembuatan Skrip Notifikasi Whatsapp

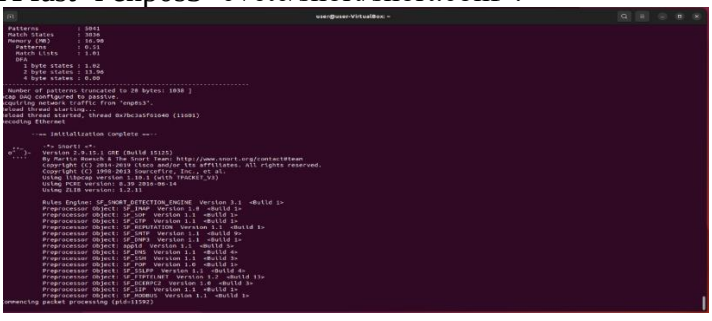
Sama seperti sebelumnya agar IDS snort dapat menjalankan skrip penulis memberikan ijin akses dengan perintah “sudo chmod +x /usr/local/bin/snort_wa_alert.py”.



Gambar 18. Pemberian Ijin Akses IDS snort

d. Menjalankan IDS Snort

Terakhir dari implementasi IDS snort dengan menggunakan telegram dan whatsapp sebagai media notifikasi, penulis menjalankan IDS snort dengan perintah “sudo snort -A fast -i enp0s3 -c /etc/snort/snort.conf”.

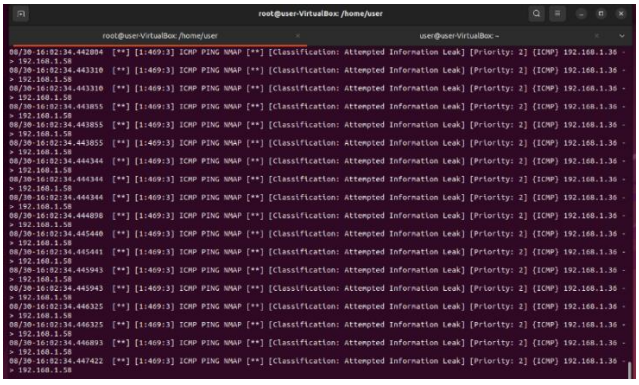


Gambar 19. IDS Snort Berjalan

5. Monitoring

Setelah penulis melakukan implementasi IDS snort dengan menggunakan telegram dan whatsapp sebagai media notifikasi pada sistem keamanan jaringan Kantor Camat Wara Kota Palopo, penulis kemudian melakukan simulasi penyerangan ke dua dengan melakukan serangan DDoS pada ubuntu menggunakan OS Kali Linux dengan aplikasi hping3. Hasil serangan dapat dilihat pada gambar dibawah ini.

Gambar 20. Melakukan Penyerangan ke Dua



Gambar 21. Hasil Deteksi IDS Snort pada Ubuntu

Berdasarkan gambar di atas penyerangan yang dilakukan dapat terdeteksi dengan mudah oleh snort pada ubuntu yang telah di IDS. Selanjutnya gambar di bawah ini merupakan hasil notifikasi yang di kirimkan oleh IDS snort ke whatsapp dan telegram ke smartphone penulis.

Gambar 22. Hasil Notifikasi IDS Snort pada Whatsapp

Gambar 23. Hasil Notifikasi IDS Snort pada Telegram

Berdasarkan hasil simulasi serangan DDoS pada ubuntu menggunakan OS Kali Linux dengan aplikasi hping3 dapat terdeteksi oleh server yang telah menggunakan IDS snort dan mengirimkan notifikasi secara realtime pada whatsapp dan telegram. dapat disimpulkan dengan menerapkan IDS snort pada ubuntu dapat memonitoring dan mendeteksi serangan DDoS yang dilakukan oleh peneliti.

KESIMPULAN

Berdasarkan hasil dari rangkaian penelitian implementasi intrusion detection system (IDS) snort sebagai sistem keamanan menggunakan whatsapp dan telegram sebagai media notifikasi di Kantor Camat Wara Kota Palopo terhadap rumusan dan batasan masalah yang ada, maka penulis dapat menyimpulkan bahwa: Pengimplementasian snort IDS menggunakan OS ubuntu 2022 dengan menginstal IDS secara langsung dari repository snort kemudian melakukan pengaturan rules dan validasi snort pada OS ubuntu. Pengitegrasian whatsapp dan telegram sebagai penerima notifikasi snort IDS dilakukan membuat boot pada masing-masing aplikasi utnuk meneriam notifikasi secara realtime. Untuk boot whatsapp menggunakan aplikasi pihak ke tiga yaitu twilio sedangkan telegram menggunakan boot father yang telah ada pada aplikasi telegram.

REFERENCES

Alamsyah, Hendri. (2022). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. Jurnal Jointeks, Vol. 5 No. 1.

Hasibuan, Marzuki. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box. Jurnal teknik Informatika, Vol. 1 No. 4.

Cinderatama, Toga. (2022). Implementasi Metode K-Means, Dbscan, dan Meanshift Untuk Analisis Jenis Ancaman Jaringan Pada Intrusion Detection System. Jurnal Inovtek Polbeng, Vol. 7 No. 1.

Purnama, Tommy. (2023). Implementasi Intrusion Detection System (IDS) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp dan Telegram Sebagai Media Notifikasi. Jurnal Ilmiah Teknologi Informasi Dan Komunikasi (JTIK), Vol 14, No.2,

Mananggel, Arther. (2021). Perancangan Jaringan Komputer di SMK Menggunakan Cisco Packet Tracer. Jurnal Pendidikan Teknologi Informasi dan Komunikasi, Vol. 1 No. 1.