JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK) VOL 14, No.2, September 2023, pp. 358 - 369
p-ISSN : 2087-0868 (media cetak)
e-ISSN : 2598-9707 (media online)
http://ejurnal.provisi.ac.id/index.php/JTIKP

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT SEBAGAI SISTEM KEAMANAN MENGGUNAKAN WHATSAPP DAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI

Tommy Purnama[1], Yusuf Muhyidin[2], Dayan Singasatia[3]
[1,2,3] Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Wastukancana Purwakarta,
[1] tommypurnama15@wastukancana.ac.id; [2] yusufmuhyidin@wastukancana.ac.id; [3] dayan@wastukancana.ac.id

ARTICLE INFO

Article history:

Received : 27 – Juli - 2023
Received in revised form : 8 – Agustus - 2023
Accepted : 29 – Agustus - 2023
Available online : 1 – September - 2023

ABSTRACT

Intrusion Detection System (IDS) is a system that functions to identify and detect attacks carried out by unauthorized parties on a network. However, some of the existing IDS systems have a deficiency in providing notifications to administrators in the event of an attack, sometimes the administrator may not be able to monitor the network all the time. This can lead to undetected attacks on the network and provide an opening for hackers to take control of the system. Therefore, it is necessary to implement IDS using WhatsApp and Telegram as Notification Media to ensure better and more effective network security. Network Development Life Cycle (NDLC) is an approach used to develop or design computer network systems. This method allows monitoring of the system being designed or developed in order to better know its performance. The NDLC method consists of 6 (six) stages, namely Analysis, Design, Simulation Prototype, Implementation, Monitoring and Management. After testing, it was concluded that IDS Snort can identify and detect various attacks, such as ping attacks (ICMP Traffic), Port Scanning, and DOS/DDOS UDP Flooding aimed at servers based on IDS rules made and also bash shell is able to record and send messages alerts when an attack occurs via WhatsApp and Telegram. The number of alert messages sent differs depending on the type of attack, the duration of the attack and also the notification media used.

***Keywords**: Intrusion Detection System (IDS),WhatsApp, Telegram, Network Development Life Cycle (NDLC),Snort, network attacks.*

1. PENDAHULUAN

Saat ini, teknologi mengalami perkembangan yang sangat cepat, terutama dengan adanya fasilitas internet yang sangat canggih. Meskipun begitu, tidak dapat diabaikan bahwa penggunaan internet juga

Received 27 – Juli - 2023; Revised 8 – Agustus - 2023; Accepted 29 – Agustus - 2023

membawa risiko dan kerugian. Salah satu contohnya adalah ancaman dari pihak-pihak yang tidak bertanggung jawab, yang sering disebut sebagai hacker. Oleh karena itu, seorang administrator jaringan harus memastikan bahwa sistem jaringan komputer tetap aman dan terlindungi dari serangan hacker[1].

Sangat penting bagi sebuah jaringan komputer untuk menjaga keamanannya dengan baik. Jika tidak, kelemahan yang ada dalam jaringan tersebut dapat memungkinkan akses tanpa izin kepada pihak yang tidak dikenal, berpotensi menyebabkan berbagai kerugian seperti kehilangan data, kerusakan pada sistem server, penurunan kualitas layanan bagi pengguna, atau bahkan kehilangan aset berharga bagi institusi.[2]. IDS merupakan sistem yang bertugas mendeteksi aktivitas yang mencurigakan di dalam suatu jaringan. [3]. Namun, beberapa sistem IDS yang ada saat ini memiliki kekurangan dalam memberikan notifikasi kepada administrator jika terjadi serangan, terkadang administrator mungkin tidak dapat memantau jaringan setiap saat. Hal ini dapat menyebabkan serangan yang tidak terdeteksi pada jaringan dan memberikan celah bagi peretas untuk mengambil kendali atas sistem. WhatsApp dan Telegram merupakan aplikasi yang digunakan untuk berkomunikasi secara real-time. Aplikasi ini juga dilengkapi dengan berbagai fitur yang memungkinkan untuk diterapkan sebagai media notifikasi bagi sistem keamanan jaringan. Dengan menggabungkan IDS dengan WhatsApp dan Telegram, diharapkan dapat meningkatkan efektivitas sistem keamanan jaringan dan memberikan notifikasi yang cepat dan tepat waktu kepada administrator jika terjadi serangan pada jaringan.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan

Keamanan jaringan merupakan suatu sistem yang bertujuan untuk mencegah aktivitas yang tidak diinginkan dengan cara mengidentifikasi pengguna yang tidak memiliki hak akses dalam jaringan. Saat menghubungkan komputer ke dalam jaringan, baik menggunakan kabel maupun nirkabel, hal ini memungkinkan orang lain untuk mengakses, mengubah, atau bahkan menghapus data yang ada dalam jaringan tersebut. Dengan pendekatan berlapis, keamanan jaringan melindungi dari ancaman yang datang dari luar dan juga dari dalam jaringan itu sendiri. Setiap organisasi memerlukan keamanan jaringan guna melindungi aset dan infrastruktur dari serangan yang dapat berkembang dengan cepat. Pengamanan jaringan dapat dilakukan dengan cara mengatur hak akses pada komputer, membatasi akses bagi pengguna tertentu pada folder dan file tertentu.Dalam konteks jaringan komputer, terdapat dua serangan yang umum dilakukan, yaitu Port Scanning dan DoS (*Denial of Service*). Port Scanning digunakan untuk mencari port yang terbuka pada jaringan guna menemukan titik lemah yang dapat dimanfaatkan. Sementara itu, DoS adalah jenis serangan di mana penyerang mengirimkan request secara berulang kali untuk menyibukkan server hingga akhirnya menyebabkan kerusakan atau kegagalan pada server tersebut. Dengan cara-cara serangan ini, penyerang dapat dengan mudah mengakses atau merusak data yang ada dalam jaringan[4].

2.2. *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) ialah sebuah sistem yang khusus dirancang untuk mengenali aktivitas yang mencurigakan pada jaringan komputer atau sistem komputer. Sistem ini bertugas memantau lalu lintas jaringan dan aktivitas sistem guna mendeteksi tanda-tanda adanya serangan atau kegiatan yang ilegal[5]. IDS menerapkan berbagai pendekatan untuk menemukan lalu lintas atau paket data yang mencurigakan dalam jaringan, yang terbagi menjadi dua jenis, yakni berbasis jaringan (NIDS) dan berbasis *host* (HIDS). Selain dua pendekatan tersebut, sistem deteksi intrusi juga menggunakan metode berbasis signature dan anomaly pada proses pendeteksian[6].

2.3. Snort

Snort adalah sebuah *software* yang berperan dalam melakukan fungsi untuk mengenali serta menganalisis tindakan yang mencurigakan didalam jaringan. Program ini dapat menangkap dan mencatat paket data yang melewati jaringan, serta dapat mengenali berbagai serangan yang berasal dari luar. Snort memiliki tiga mode operasi yaitu Paket Sniffer, berfungsi untuk melihat paket yang sedang berjalan di jaringan. Paket Logger, berfungsi untuk menyimpan seluruh paket yang lewat di jaringan untuk dianalisis di kemudian hari. NIDS (*Network Intrusion Detection System*), dalam mode ini, Snort berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer[7].

2.4. WhatsApp

WhatsApp adalah sebuah aplikasi pesan yang dapat digunakan di berbagai platform. WhatsApp juga memungkinkan penggunanya untuk mengirim pesan tanpa perlu membayar biaya tambahan untuk SMS. Hal ini disebabkan karena aplikasi ini menggunakan paket data internet yang sama seperti saat mengirim

p-ISSN : e-ISSN :

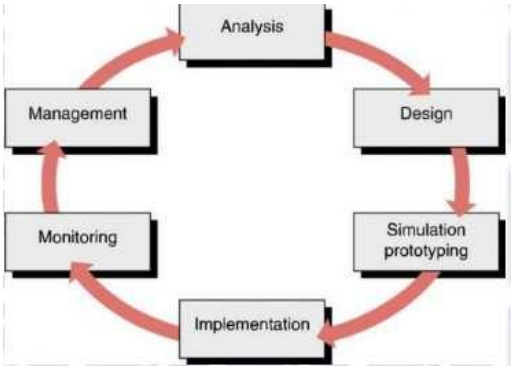
email atau menjelajah web. Selain itu, WhatsApp juga dikenal sebagai aplikasi pesan instan yang paling populer di dunia, dengan jumlah pengguna yang sangat banyak. Di dalam WhatsApp, pengguna dapat melakukan berbagai hal, seperti mengirim pesan teks, gambar, video, serta melakukan panggilan video. Selain itu, WhatsApp juga memungkinkan pembuatan kelompok diskusi untuk berkomunikasi dengan lebih banyak orang secara bersamaan.

2.5. Telegram

Telegram adalah sebuah aplikasi yang menggunakan teknologi cloud, sehingga memungkinkan penggunanya untuk mengakses satu akun Telegram dari beberapa perangkat sekaligus. Selain itu, pengguna juga bisa dengan mudah berbagi berkas sampai 1,5 GB. Aplikasi Telegram dibuat oleh dua saudara asal Rusia, yaitu Nikolai Durov dan Pavel Durov. Mereka bekerja sama dalam peran yang berbeda. Nikolai bertanggung jawab atas pengembangan aplikasi, termasuk menciptakan protokol MTProto yang menjadi inti dari Telegram. Di sisi lain, Pavel fokus pada aspek pendanaan dan infrastruktur melalui Digital Fortress[8].

2.6. *Network Development Life Cycle* (NDLC)

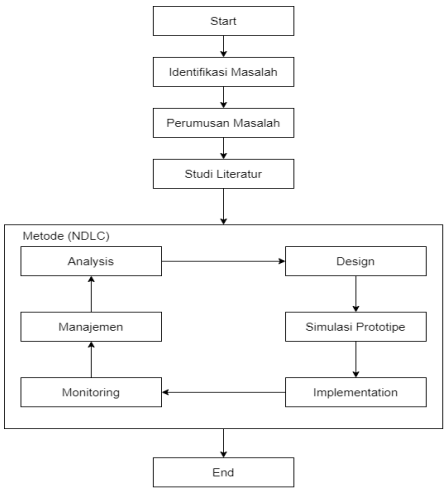
Metode Pengembangan Siklus NDLC adalah cara merancang dan mengembangkan sistem jaringan komputer, serta memantau kinerjanya. NDLC juga mengandalkan proses pembangunan sebelumnya, seperti perencanaan strategi bisnis, siklus pengembangan aplikasi, dan analisis distribusi data. Hal ini bertujuan agar sistem yang sedang dirancang atau dikembangkan dapat dipantau dengan baik[9]. Metode NDLC terdiri dari enam tahapan utama yang berfungsi sebagai panduan dalam menerapkan prosesnya. Tahapan-tahapan tersebut meliputi *Analysis, Design, Simulation Prototype, Implementation, Monitoring dan Management* [10].



Gambar2.1. Metode (NDLC)

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan Metodologi *Network Development Life Cycle* (NDLC) yang terdiri dari enam tahapan: *Analysis, Design, Simulation Prototype, Implementation, Monitoring dan Management*. Namun, penelitian ini hanya berfokus sampai pada tahap Implementasi saja. Berikut ini adalah kerangka penelitian yang menggambarkan penggunaan metode NDLC:



Gambar 3.1. Kerangka Penelitian

3.1 Identifikasi Masalah

Pada tahap ini dilakukan pengidentifikasian masalah yang melibatkan proses analisis menyeluruh terhadap permasalahan utama yang sudah dijelaskan dalam latar belakang masalah. Setelah masalah utama teridentifikasi, langkah selanjutnya adalah mencari solusi yang sesuai dan tepat untuk mengatasi permasalahan tersebut. Proses ini mencakup pengujian hipotesis, pengumpulan serta analisis data, dan mungkin dilanjutkan dengan eksperimen atau penelitian lebih lanjut. Tujuannya adalah menemukan solusi yang relevan dan dapat memberikan kontribusi pada pemahaman serta penyelesaian masalah yang dihadapi.

3.2 Perumusan Masalah

Pada tahap ini, dilakukan pengkajian terhadap berbagai masalah yang terkait dengan objek penelitian. Tujuan dari pengkajian ini adalah untuk merumuskan masalah-masalah tersebut yang membuat pelaksanaan penelitian dapat berjalan dengan baik.

3.3 Studi Literatur

Pada tahap ini, data dan informasi dikumpulkan dari berbagai sumber yang relevan dengan penelitian, termasuk buku, jurnal, dan materi bacaan elektronik. Langkah ini sangat penting karena membantu peneliti memperluas pemahaman tentang topik yang sedang diteliti, mengidentifikasi kerangka teoritis yang relevan, dan mendapatkan wawasan mendalam tentang isu yang sedang diteliti.

3.4 Analisis

Pada tahap ini, dilakukan analisis permasalahan terkait dengan penelitian untuk menentukan kebutuhan sistem, termasuk perangkat keras, perangkat lunak server, klien, dan aplikasi lainnya. Tahap ini dapat disebut sebagai tahap pengumpulan data yang diperlukan untuk merumuskan masalah dan mengatasi kendala yang ada.

3.5 *Design*

Pada tahap ini, dilakukan proses perancangan gambaran topologi jaringan. dan sistem keamanannya berskala kecil antara server dan attacker terdapat gambaran bagaimana sistem ids ini bekerja ketika belum menerapkan whatsapp dan telegram sebagai mendia notifaksi dan ketika sudah menerapkan.

3.6 Simulasi prototipe

Pada tahap ini, dilakukan persiapan untuk menginstal dan mengkonfigurasi Twilio, bot Telegram dan IDS Snort, serta membuat script bash shell agar nantinya pemberitahuan tentang serangan dapat dikirimkan melalui WhatsApp dan Telegram.

3.7 Implementasi

Pada tahap ini dilakukannya penerapan dan pengujian terhadap sistem keamanan jaringan komputer berbasis virtual private server menggunakan Ubuntu Desktop sebagai server dan Kali Linux sebagai attacker. Pengujian ini bertujuan untuk memastikan bahwa sistem IDS Snort dapat berfungsi dengan baik saat terjadi serangan dan mampu mengirimkan notifikasi melalui aplikasi WhatsApp dan Telegram.

4. HASIL DAN PEMBAHASAN

4.1 Analisis

Pada tahap analisis ini, peneliti melakukan pengidentifikasian permasalahan, merumuskan masalah, dan mengumpulkan data atau informasi terkait penelitian. Tujuan dari langkah ini adalah untuk memastikan bahwa sistem yang akan diterapkan dapat berjalan dengan baik nantinya.

a) Identifikasi Masalah

Sistem Deteksi Intrusi (IDS) berfungsi untuk menemukan serangan yang dilakukan oleh pihak yang tidak berwenang pada jaringan. Meskipun demikian, beberapa Sistem IDS yang ada saat ini memiliki kekurangan dalam memberikan pemberitahuan kepada administrator saat terjadi serangan. Terkadang, administrator tidak dapat memantau jaringan secara terus-menerus. Situasi ini berpotensi menyebabkan serangan tidak terdeteksi pada jaringan dan memberikan peluang bagi peretas untuk mengambil alih kontrol sistem. Maka dari itu perlu adanya sistem IDS yang mampu memberikan pemberitahuan serangan secara realtime agar administrator jaringan dapat mengantisipasi ketika terjadi adanya serangan.

b) Perumusan Masalah

Berdasarkan identifikasi masalah diatas maka perumusan masalahnya adalah bagaimana cara membangun sistem *INTRUSION DETECTION SYSTEM* (IDS) dengan notifikasi secara realtime menggunakan Whatsapp dan Telegram sebagai media notifikasi?

p-ISSN : e-ISSN :

c) Studi Literatur

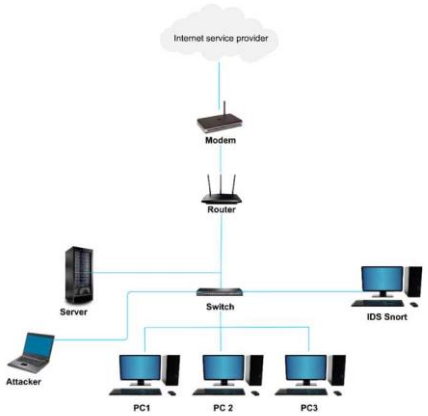
Dalam penelitian ini, peneliti mengumpulkan data dan informasi dari berbagai sumber terpercaya seperti jurnal, artikel ilmiah, dan sumber lain yang relevan dengan topik penelitian. Setelah data terkumpul dilakukanlah analisis terhadap setiap referensi yang telah dikumpulkan. Analisis ini meliputi membaca secara menyeluruh dan memahami konten dari setiap studi literatur, mencatat temuan-temuan penting, serta mengidentifikasi kerangka pemikiran dan metodologi yang digunakan dalam penelitian sebelumnya. Hal ini akan memberikan pemahaman yang lebih mendalam tentang implementasi IDS dengan menggunakan WhatsApp dan Telegram sebagai media notifikasi. Peneliti dapat mempelajari konsep integrasi kedua platform tersebut, mengidentifikasi kelebihan dan kekurangan penggunaan mereka, mengevaluasi kinerja dan kehandalan notifikasi yang dikirim melalui kedua media tersebut, serta menemukan temuan-temuan penting dari penelitian terdahulu. Agar memberikan pemahaman tentang konsep implementasi *Intrusion Detection System* (IDS) dengan memanfaatkan WhatsApp dan Telegram sebagai media notifikasi.

4.2 Design

Pada tahap desain ini, merupakan kelanjutan dari tahap sebelumnya yang telah menjelaskan dan memberikan gambaran tentang sistem yang akan diterapkan, perancangan sistem yang akan dibangun direpresentasikan dalam bentuk topologi gambar seperti berikut:

a) Design Topologi Awal

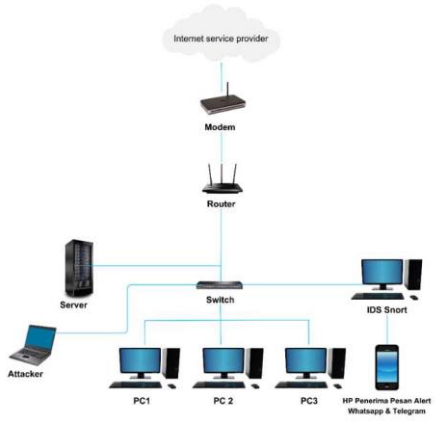
Design topologi awal ini merupakan alur sistem *Intrusion Detection System* (IDS) snort yang dimana ketika dilakukan penyerangan maka IDS snort tidak akan mengirimkan pesan pemberitahuan ke whatsapp dan telegram yang dapat mengakibatkan keterlambatan dalam mengambil tindakan untuk menghentikan serangan atau membatasi dampaknya terhadap jaringan.



Gambar 4.1. Topologi Awal

b) Design Topologi Yang Diusulkan

Design topologi yang diusulkan ini penulis mengusulkan penerapan *Intrusion Detection System* (IDS) snort menggunakan pemberitahuan serangan ke whatsapp dan telegram guna memberikan pemberitahuan secara instan ketika terjadi serangan atau aktivitas mencurigakan dalam jaringan. yang memungkinkan untuk merespons dengan cepat dan mengambil tindakan pencegahan, mengurangi risiko potensial dan dampak yang mungkin ditimbulkan oleh serangan.



Gambar 4.2. Topologi Usulan

4.3 *Simulation Prototype*

Pada tahap ini penulis melakukan persiapan simulasi lansung untuk penerapan *Intrusion Detection System* (IDS) snort notifikasi whatsapp dan telegram dengan menggunakan sistem operasi Ubuntu Desktop sebagai server dan pembuatan script bash shell agar nantinya notifikasi serangan bisa terkirim ke whatsapp dan telegram.

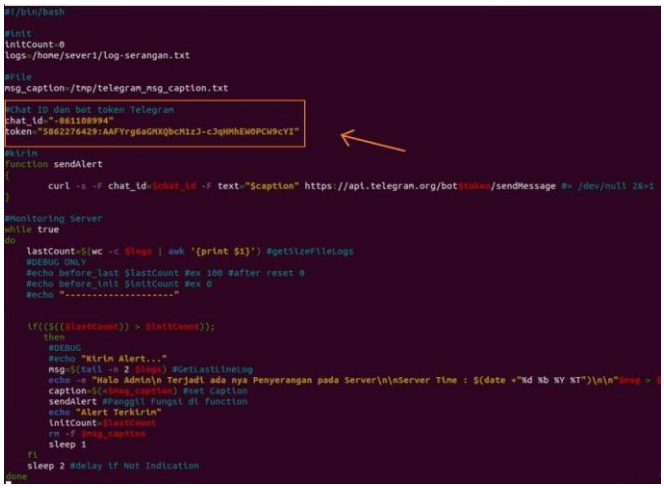
4.3.1 Konfigusi IDS Snort

a) apt-get install snort -y (menginstall snort)
b) cd /etc/snort/rules (masuk kedirektori rules)
c) nano local.rules (Tambahkan Rules IDS Snort)
   - alert icmp any any -> $HOME_NET any (msg:"Ada yang melakukan ping"; sid:10000013; rev:1; classtype:icmp-event;)
   - alert tcp any any -> $HOME_NET any (msg:"Ada yang melakukan Port Scanning"; detection_filter:track by_src, count 30, seconds 60; sid:1000006; rev:2;)
   - alert udp any any -> $HOME_NET any (msg:"UDP Flooding"; detection_filter:track by_src, count 30, seconds 60; sid:1000008; rev:2;)
d) snort -c /etc/snort/snort.conf -i enp0s3 -A console
e) snort -i enp0s3 -c /etc/snort/snort.conf -l /var/log/snort -d -A console > /home/sever1/log-serangan.txt

4.3.2 Pembuatan Bash Shell Telegram

Pembuatan script bash shell telegram dapat membantu mengintegrasikan sistem keamanan ids snort dengan layanan pesan instan telegram.

a) nano tele-bot.sh
b) chmod 777 tele-bot.sh (Memberi Ijin Modifikasi tele-bot.sh)
c) Selanjutnya, buatlah script bash shell dengan mengisikan chat id dan token yang diperoleh dari pembuatan bot Telegram.



Gambar 4.3. Bash Shell Telegram

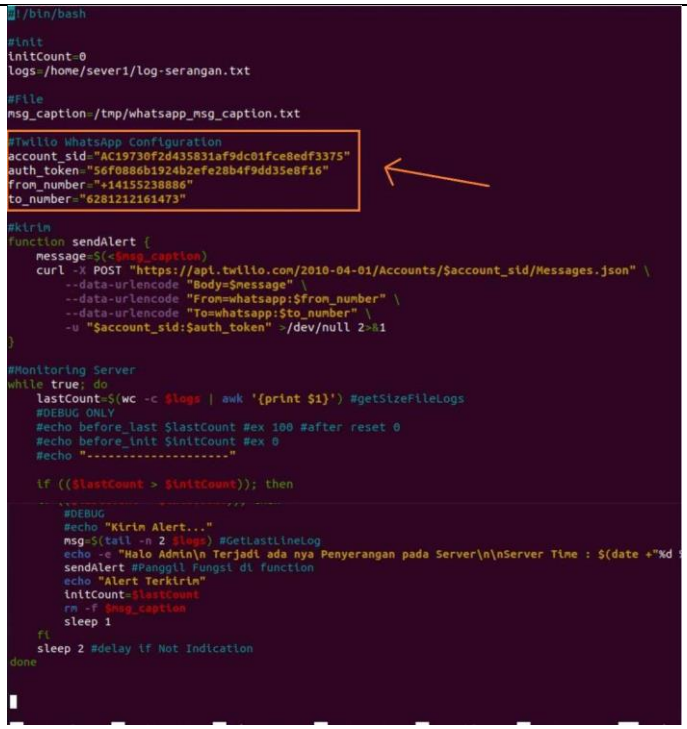
Pada gambar di atas, merupakan script bash shell yang berisi token API key dan Chat ID. Script ini berfungsi untuk membaca log serangan yang berjalan di IDS Snort dan mengirimkan pemberitahuan serangan ke telegram. Tujuannya adalah untuk melakukan monitoring dan pendeteksian terhadap serangan pada server Ubuntu Desktop.

4.3.3 Pembuatan Bash Shell WhatsApp

p-ISSN : e-ISSN :

Pembuatan script bash shell whatsapp dapat membantu mengintegrasikan sistem keamanan ids snort dengan layanan pesan instan whatsapp.

a) nano wa-bot.sh
b) chmod 777 tele-bot.sh (Memberi Ijin Modifikasi tele-bot.sh)
c) lalu buat script bash shell dengan memasukan sid, token, nomber twilio yang didapatkan dari pembuatan akun whatsapp API twilio dan masukan nomer whatsapp tujuan yang akan dikirimkan notifikasi serangan.



Gambar 4.4. Bash Shell WhatsApp

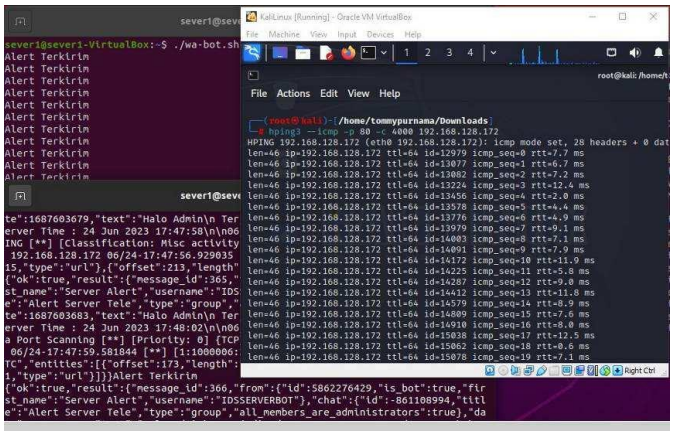
Pada gambar di atas, terdapat script bash shell yang memuat SID, Token, Nomor Twilio, dan nomor WhatsApp yang akan digunakan untuk menerima notifikasi serangan. Script ini berfungsi untuk membaca log serangan yang berjalan di IDS Snort serta mengirimkan pemberitahuan tentang serangan tersebut melalui aplikasi whatsapp.

4.4 Implementasi

Dalam tahap ini peneliti melakukan impelementasi System keamanan jaringan berbasis virtual private server untuk mengetahui apakah ids snort berhasil atau tidak ketika dimplimentasikan dengan aplikasi whatsapp dan telegram untuk pemberitahuan notifikasi serangan agar mempermudah dalam mengamankan jaringan.

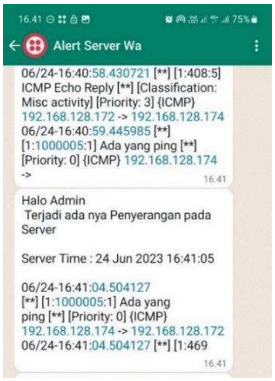
4.4.1 Ping Attack (ICMP Traffic)

Percobaan Serangan Ping Attack (ICMP Traffic) untuk mengatuhi peyerang dan target bisa saling berkomunikasi satu sama lain .



Gambar 4.5. Pengujian Serangan Ping Attack

Pada gambar terlihat bahwa penyerang mencoba melakukan serangan ke target dengan IP 192.168.128.172. Dimana penyerang mengirimkan permintaan ping ICMP yang berulang (reply) ke server. Namun, di dalam jaringan komputer yang menggunakan *Intrusion Detection System* (IDS) di Ubuntu Desktop, upaya serangan ini berhasil terdeteksi dan bash shell yang sedang berjalan akan membaca log serangan ids dari serangan ping attack tersebut lalu memberikan pemberitahuan serangan ke wahatsapp dan telegram.



Gambar 4.6. Ping Attack Notifikasi Whatsapp

Pada Gambar diatas merupakan pemberitahuan dari serangan ping attack yang terkirim ke aplikasi whatsapp.

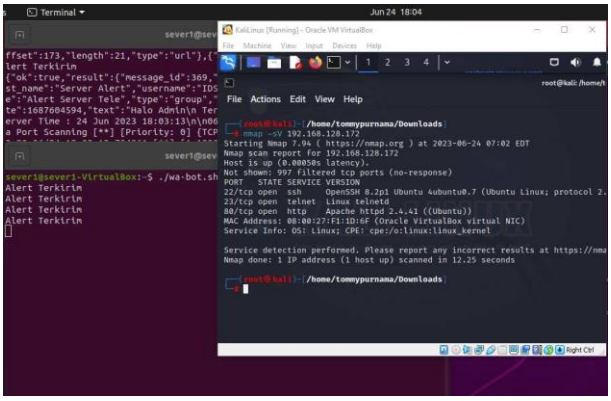
Gambar 4.7. Ping Attack Sesudah Diterapkan Notifikasi Telegram

Pada Gambar diatas merupakan pemberitahuan dari serangan ping attack yang terkirim ke aplikasi telegram.

p-ISSN : e-ISSN :

4.4.2 *Port Scanning*

Pada tahap percobaan selanjutnya, penyerang akan melakukan pemindaian atau *scanning* terhadap jaringan komputer yang menjadi target.



Gambar 4.8. Pengujian Serangan *Port Scanning*

Pada gambar di atas, Penyerang berhasil melakukan pemindaian port (*port scanning*) terhadap jaringan komputer yang menjadi target dengan IP 192.168.128.172 menggunakan *tools* nmap dan Komputer yang telah d iterapkan IDS Snort berhasil mendeteksi aktivitas nmap (port scanning) terhadap jaringan komputer, sebagai responsnya, bash shell akan memberikan pemberitahuan mengenai kegiatan scanning tersebut melalui WhatsApp dan Telegram.

Gambar 4.9. Port Scaning Sesudah Diterapkan Notifikasi WhatsApp

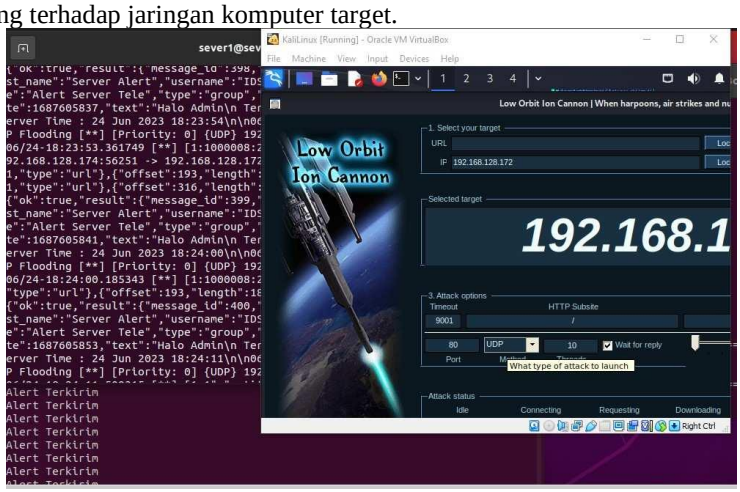
Pada Gambar diatas merupakan pemberitahuan dari aktivitas port scanning yang terkirim ke aplikasi whatsapp.

Gambar 4.10. Port Scaning Sesudah Diterapkan Notifikasi Telegram

Pada Gambar diatas merupakan pemberitahuan dari aktivitas port scanning yang terkirim ke aplikasi telegram.

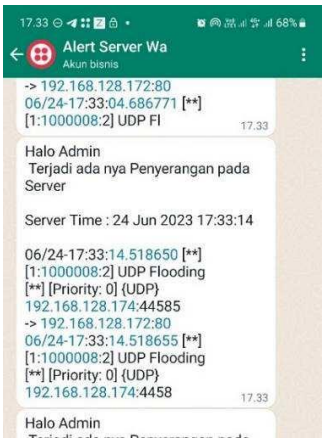
4.4.3 DDOS (UDP Flooding)

Pada Percobaan selanjutnya akan dilakukannya serangan DDOS (UDP Flooding) menggunakan LOIC dari penyerang terhadap jaringan komputer target.



Gambar 4.11. Pengujian Serangan DDOS UDP Flooding

Pada gambar di atas merupakan penyerangan DDoS (UDP Flooding) terhadap jaringan target dengan alamat IP tujuan 192.168.128.172. Serangan ini ditujukan ke port 80 dengan menggunakan protokol UDP. IDS Snort berhasil mendeteksi serangan DDoS tersebut, dan sebagai tindakan respons, bash shell akan mengirimkan pemberitahuan mengenai serangan ke WhatsApp dan Telegram.



Gambar 4.12. DDOS UDP Flooding Sesudah Diterapkan Notifikasi WhatsApp

Pada Gambar diatas merupakan pemberitahuan serangan DDOS (UDP Flooding) yang terkirim ke aplikasi whatsapp.

p-ISSN : e-ISSN :

Gambar 4.13. DDOS UDP Flooding Sesudah Diterapkan Notifikasi Telegram

Pada Gambar diatas merupakan pemberitahuan serangan DDOS (UDP Flooding) yang terkirim ke aplikasi telegram.

4.5 Hasil Kemampuan Deteksi Sistem Keamanan

Tabel 4.1. Hasil Kemampuan Deteksi Sistem Keamanan

No	Sistem Keamanan	Dapat Mendeteksi Serangan			Terkirim Notifikasi	
		Ping Attack	Port Scaning	DDOS Attack	WhatsApp	Telegram
1	Snort	Bisa	Bisa	Bisa	Bisa	Bisa

Dari hasil pengujian snort dapat mendeteksi semua serangan seperti ping attack, Port Scaning dan DDOS Attack dan dapat mengirimkan notifikasi serangan kedua aplikasi pesan tersebut.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Setelah dilakukan pengujian, disimpulkan bahwa IDS Snort dapat mengidentifikasi dan mendeteksi berbagai serangan, seperti ping attack (ICMP Traffic), Port Scanning, serta DOS/DDOS UDP Flooding yang ditujukan ke server, dengan sistem operasi Ubuntu Desktop 20.04.2 LTS berdasarkan rules IDS Snort yang dibuat dan juga bash shell mampu merekam dan mengirimkan pesan pemberitahuan secara langsung saat terdeteksi adanya serangan ke aplikasi whatsapp dan telegram. ini sangat berguna karena memungkinkan administrator untuk merespons dengan cepat dan mengambil tindakan yang diperlukan untuk melindungi jaringan.

5.2. Saran

Saran yang dapat diberikan berdasarkan hasil penelitian ini adalah sebagai berikut:

1. Penting untuk mempertimbangkan penggunaan lebih dari satu media notifikasi sebagai lapisan keamanan tambahan. Selain WhatsApp dan Telegram, mungkin juga perlu mempertimbangkan penggunaan email, pesan teks, atau platform lainnya untuk memastikan pesan peringatan serangan intrusi dapat segera diterima oleh administrator.
2. Penambahan IPS *(Intrusion Prevention System*) agar ketika terjadi serangan dapat dilakukan pemblokiran.

6. DAFTAR PUSTAKA

[1] W. W. Purba and R. Efendi, “Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT,” *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[2] R. W. Ismail and R. Pramudita, “Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi,” *J. Mhs. Bina Insa.*, vol. 5, no. 1, pp.

53–62, 2020.

[3] B. Fachri and F. H. Harahap, “Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer,” *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[4] K. Al Fikri and Djuniadi, “Keamanan Jaringan Menggunakan Switch Port Security,” *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 2, pp. 302–307, 2021, [Online]. Available: http://bit.ly/InfoTekJar

[5] 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.

[6] S. Alviana and I. D. Sumitra, “Analisis Pengukuran Penggunaan Sumber Daya Komputer Pada Intrusion Detection System Dalam Meminimalkan Serangan Jaringan,” *Komputa J. Ilm. Komput. dan Inform.*, vol. 7, no. 1, pp. 27–34, 2018, doi: 10.34010/komputa.v7i1.2533.

[7] J. D. Santoso, “Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System,” *Infos*, vol. 1, no. 3, pp. 44–50, 2019.

[8] A. Fitriansyah, Fifit, “Penggunaan Telegram Sebagai Media Komunikasi Dalam Pembelajaran Online,” *J. Hum. Bina Sarana Inform.*, vol. 20, no. Cakrawala-Jurnal Humaniora, p. 113, 2020, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala

[9] U. A. Ahmad, R. E. Saputra, and P. Y. Pangestu, “Perancangan Infrastruktur Jaringan Komputer Menggunakan Fiber Optik Dengan Metode Network Development Life Cycle (NDLC),” *eProceedings …*, vol. 8, no. 6, pp. 12066–12079, 2021, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17035%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17035/16748

[10] N. Nurdadyansyah and M. Hasibuan, “Tampilan Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah,” *Konf. Nas. Ilmu Komput.*, pp. 342–346, 2021, [Online]. Available: https://prosiding.konik.id/index.php/konik/article/view/75/68