RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

Perancangan Sistem Bot Alert Telegram Sebagai Notifikasi Deteksi Serangan Ping of Death Berbasis Snort

Dicky Rachman Juliandi[1], Joni Karman[2,*], Rusdiyanto[3]

[1]Fakultas Ilmu Teknik, Prodi Rekayasa Sistem Komputer, Universitas Bina Insan, Lubuklinggau, Indonesia
[2]Fakultas Ilmu Teknik, Prodi Sistem Informasi, Universitas Bina Insan, Lubuklinggau, Indonesia
[3]Fakultas Ilmu Teknik, Prodi Informatika, Universitas Bina Insan, Lubuklinggau, Indonesia
Email: [1]901020032@mhs.univbinainsa.ac.id, [2,*]joni_karman@univbinainsan.ac.id, [3]rusdiyanto@univbinainsan.ac.id
Email Penulis Korespondensi: joni_karman@univbinainsan.ac.id

Abstrak−Serangan Ping of Death adalah jenis serangan penolakan layanan (DoS) yang mengeksploitasi kerentanan di Internet Control Message Protocol (ICMP). Serangan ini dilakukan dengan cara mengirimkan ping dalam jumlah besar hingga melampaui batas maksimum yang diperbolehkan oleh jaringan sehingga menyebabkan server atau perangkat jaringan menjadi lambat atau bahkan tidak responsif. Serangan ini dapat berdampak parah terhadap kinerja server dan jaringan, terutama untuk layanan yang memerlukan ketersediaan tinggi seperti server Sinanan Lubuklinggau. Penelitian ini bertujuan untuk merancang sistem alert Telegram Bot sebagai sarana notifikasi otomatis untuk mendeteksi serangan Ping of Death pada server Sinanan Lubuklinggau, menggunakan Snort, sebuah software sistem deteksi yang sedang menyusup ke jaringan "NIDS". Snort digunakan untuk mendeteksi serangan dengan memeriksa paket data yang melewati jaringan. Jika Snort mendeteksi aktivitas mencurigakan seperti serangan Ping of Death, sistem akan langsung mengirimkan peringatan melalui bot Telegram. Peringatan tersebut berisi informasi rinci tentang serangan tersebut, termasuk alamat IP, penyerang, stempel waktu, dan lokasi jaringan yang terpengaruh. Sistem ini juga telah terbukti bekerja dengan baik di lingkungan jaringan dengan lalu lintas tinggi tanpa mengganggu kinerja server. Dengan menerapkan sistem ini, administrator jaringan dapat bertindak lebih cepat untuk mencegah dan mengelola ancaman serangan Ping of Death, sehingga menjaga stabilitas dan keamanan server Sinanan Lubuklinggau.

Kata Kunci: Ping of Death; Internet Control Message Protocol (ICMP); Server; Snort; Telegram

Abstract−The Ping of Death attack is a type of denial of service (DoS) attack that exploits a vulnerability in the Internet Control Message Protocol (ICMP). This attack is carried out by sending a large number of pings that exceed the maximum limit allowed by the network, causing the server or network device to become slow or even unresponsive. This attack can have a severe impact on server and network performance, especially for services that require high availability such as the Sinanan Lubuklinggau server. This research aims to design a Telegram Bot alert system as an automatic notification tool to detect Ping of Death attacks on the Sinanan Lubuklinggau server, using Snort, a detection system software that is infiltrating the "NIDS" network. Snort is used to detect attacks by examining data packets passing through the network. If Snort detects suspicious activity such as a Ping of Death attack, the system will immediately send an alert via the Telegram bot. The alert contains detailed information about the attack, including the IP address, attacker, timestamp, and location of the affected network. This system has also been proven to work well in high-traffic network environments without disrupting server performance. By implementing this system, network administrators can act more quickly to prevent and manage the threat of Ping of Death attacks, thereby maintaining the stability and security of the Sinanan Lubuklinggau server.

Keywords: Ping of Death; Internet Control Message Protocol (ICMP); Server; Snort; Telegram

1. PENDAHULUAN

Pada era globalisasi saat ini, Teknologi Informasi (TI) berkembang sangat pesat dengan adanya jaringan internet yang mempermudah komunikasi dan akses informasi. Namun, perkembangan ini juga menimbulkan masalah baru, yakni penyalahgunaan informasi atau data penting oleh pihak yang tidak bertanggung jawab untuk kepentingan pribadi[1]. Keamanan merupakan salah satu masalah terbesar bagi pengguna Internet terutama penyedia sebuah server maupun sistem jaringan komputer. Masalah tersebut menimbulkan kecenderungan besar untuk memiliki Intrussion Detection System (IDS) pada setiap jaringan. IDS merupakan perangkat lunak atau perangkat keras sistem yang secara otomatis melakukan proses pemantauan (monitoring) insiden yang terjadi dalam sistem komputer atau jaringan serta menganalisis tanda- tanda adanya masalah terhadap keamanan sistem[2][3]. Hal ini mengakibatkan perlunya sistem keamanan jaringan yang semakin kuat, terutama bagi penyedia server dan sistem jaringan komputer. Salah satu contohnya adalah server aplikasi SINANAN, yang dikembangkan oleh Dinas Kominfo Kota Lubuklinggau sebagai sistem informasi pengelolaan data kepegawaian dan Sumber Daya Manusia (SDM) di Kota Lubuklinggau. Permasalahan yang ada terletak pada tingkat keamanan server aplikasi SINANAN yang belum optimal, dimana saat ini belum ada penerapan sistem keamanan pada server, sehingga memungkinkan terjadinya serangan pada server SINANAN tersebut, sedangkan aplikasi tersebut sangat dibutuhkan setiap saat karena seluruh Aparat Sipil Negara (ASN) Kota Lubuklinggau, karena hanya melalui aplikasi tersebut untuk pengurusan yang terkait dengan kepegawaian serta SDM (Sumber Daya Manusia) dari ASN dipemerintahan kota Lubuklinggau.

Salah satu solusi yang diharapkan dapat mengatasi permasalahan ini adalah dengan menerapkan Intrusion Detection System (IDS) berbasis Snort, sebuah perangkat yang mampu mendeteksi aktivitas mencurigakan pada jaringan. IDS (Intrusion Detection System) dapat didefinisikan sebagai alat yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan komputer Dengan integrasi bot Telegram, notifikasi otomatis akan dikirimkan kepada administrator server jika terjadi ancaman atau aktivitas yang mencurigakan[4][5]. Hal ini akan mempermudah pengelolaan keamanan server dan mencegah kerusakan lebih lanjut. Penggunaan Snort dalam sistem

RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

deteksi serangan dapat membantu mengidentifikasi aktivitas yang mencurigakan atau potensial serangan siber, dan memanfaatkan media telegram sebagai media notifikasi jika terjadi serangan atau aktifitas jaringan yang mencurigakan, telegram akan mengirimkan notifikasi serangan tersebut kepada admininstrator jaringan yang bertanggung jawab terhadap keamanan dari aplikasi SINANAN tersebut[6][7].

Berbagai penelitian sebelumnya telah membahas penerapan sistem keamanan jaringan menggunakan Intrusion Detection System (IDS) dan integrasinya dengan berbagai media notifikasi. Misalnya, penelitian yang dilakukan oleh Sutarti, 2018 dengan judul "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal" hasil dari penelitian ini snort dapat mengetahui apa yang sedang terjadi yang di hasilkan pada alert seperti serangan Ping Of Death dan Port Scan. Pada PfSense menampilkan alert jika ada seseorang yang mencoba menyalahgunakan jaringan seperti mengakses sosial media facebook, youtube, twitter dan lain-lain bisa menindak lanjuti dengan mem-block secara otomatis[8]. Penelitian yang dilakukan Benny Wijaya, 2020 dengan judul "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort" hasil dari penelitian ini.

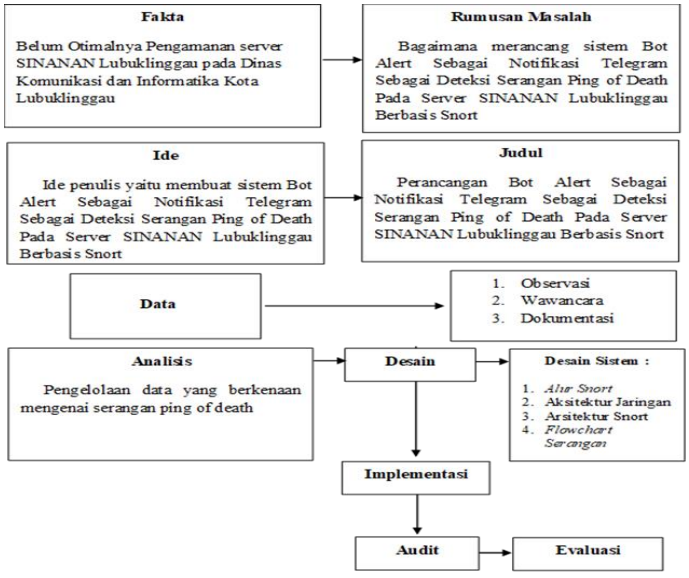
Dengan menggunakan Metode Intrusion Detection System (IDS) berbasis Snort administrator jaringan bisa mengetahui aliran paket-paket yang keluar masuk sistem, IDS akan merekam semua aktifitas tersebut dan memberikan laporan paket-paket yang mencurigakan sehingga administrator jaringan dapat mengetahui jika ada serangan yang masuk kedalam jaringan[9]. Penelitian yang dilakukan Givan Yandiputra Sunardi, 2024 dengan judul "Sistem Monitoring Serangan Jaringan Menggunakan Intrusion Detection System (IDS) Dengan Notifikasi Telegram" hasil dari penelitian ini Intrusion Detection System (IDS) dapat memonitor serangan jaringan secara real-time, meskipun ada sedikit delay dari waktu serangan terjadi hingga notifikasi terkirim ke Telegram. IDS mampu mendeteksi serangan seperti Port Scanning, Denial of Service, dan Bruteforce berdasarkan aturan yang dibuat, sehingga membantu meningkatkan keamanan jaringan dengan memberi administrator waktu untuk melakukan tindakan pencegahan[10]. Penelitian yang dilakukan Budi Sudradjat, 2017 dengan judul "Sistem Pendeteksian Dan Pencegahan Penyusup Pada jaringan Komputer Dengan Menggunakan Snort Dan Firewall" hasil dari penelitian ini Pemilihan teknologi Intrusion Detection System dan firewall sangat tepat, karena mem-filter IP address yang lewat[11]. Selanjutnya penelitian yang dilakukan oleh Daniel Desma Mahendra, 2022 dengan judul "Sistem Deteksi dan Pengendalian Serangan Denial of Service pada Server Berbasis Snort dan Telegram-API" penelitian ini menghasilkan mekanisme sistem pemantauan dan pengendalian terhadap serangan DoS melalui pengkolaborasian metode intrusion detection system (IDS) dan intrusion prevention system (IPS). Pengintegrasian Snort sebagai IDS dan Telegram-API sebagai IPS diusulkan untuk meningkatkan keamanan pada lingkungan server[12].

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem IDS berbasis Snort yang terintegrasi dengan notifikasi bot Telegram untuk mendeteksi serangan pada server SINANAN. Harapannya, sistem ini dapat meningkatkan tingkat keamanan server SINANAN dan meminimalkan risiko gangguan pada aplikasi, sehingga operasional aplikasi dapat berjalan dengan lancar.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Tahapan penelitian ini di proses berdasarkan fakta yang ada di lapangan dimana kondisinya yaitu belum optimalnya Pengamanan Server SINANAN Lubuklinggau pada Dinas Komunikasi dan Informatika Kota Lubuklinggau. Gambaran tahapan tersebut dapat dilihat pada gambar 1 berikut ini :



Gambar 1. Alur tahapan Penelitian

RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

Tahapan pertama yang di lakukan yaitu merumuskan masalah, kemudian menentukan ide. Setelah di dapat ide barulah dilakukan pengumpulan data, dalam penelitian ini dilakukan dalam berbagai metode yaitu, metode (Observasi), merupakan suatu cara pengumpulan data dengan melakukan peninjauan secara langsung terhadap objek yang diteliti[13].

Pada penelitian ini dalam mengumpulkan data-data yang diperlukan penulis melakukan pengamatan secara langsung di kantor BKPSDM dan Diskominfo Kota Lubuklinggau. Selanjutnya metode wawancara, Penulis mengadakan wawancara dan tanya jawab secara langsung kepada pegawai yang bekerja di kantor Dinas Kominfo kota Lubulinggau berkaitan dengan server SINANAN Lubuklinggau. Dan yang terakhir adalah metode Metode pustaka, Pada metode ini penulis membaca dan mencatat data yang ada pada suatu buku, jurnal dan literatur yang berhubungan dengan permasalahan yang diangkat. Setelah data terkumpil maka dilakukan lah analisis, baru kemudian dibentuklah desainya, setelah desain siap maka dilakukan uji coba terhadap desain atau implementasi desain baru kemudian dilakukan audit dan evaluasi terhadap desain tersebut.

2.2 Metode Pengembangan Sistem

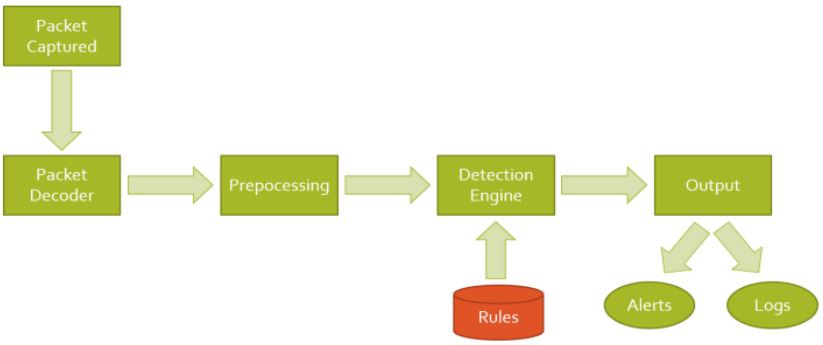
Metodologi yang digunakan dalam penelitian ini adalah Security Policy Development Life Cycle (SPDLC)[14]. Tahap-tahap yang dilakukan dalam penelitian ini yaitu, tahap pertama adalah Identifikasi, yang dilakukan untuk menemukan berbagai masalah keamanan yang dihadapi jaringan saat ini, serta memahami bagaimana sistem yang berjalan di Dinas Kominfo Kota Lubuklinggau. Selanjutnya, pada tahap Analisis, data yang diperoleh dari tahap identifikasi dianalisis untuk memahami kebutuhan pengguna pada Server SINANAN di Lubuklinggau. Pada tahap Desain, dibuat rancangan topologi sistem keamanan yang akan dibangun, termasuk alur sistem autentikasi, serta kebutuhan sistem baik dari segi perangkat lunak maupun perangkat keras. Tahap ini diikuti dengan Implementasi, yaitu penerapan hasil perancangan yang telah dilakukan. Namun, karena keterbatasan izin dari perusahaan untuk melakukan implementasi secara langsung, hasil rancangan disimulasikan pada jaringan yang lebih kecil, dimulai dengan instalasi perangkat dan konfigurasi perangkat lunak serta perangkat keras yang diperlukan. Selanjutnya, pada tahap Audit, sistem yang disimulasikan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal. Tahap ini dilakukan melalui skenario pengujian. Terakhir, pada tahap Evaluasi, dilakukan analisis hasil pengujian untuk mengukur efektivitas teknologi keamanan yang dibangun, membandingkannya dengan tujuan awal, dan memberikan saran perbaikan untuk masa yang akan datang[15].

2.3 Analisis Kebutuhan dan Desain Sistem

Penulis telah menganalisa kebutuhan sistem di Dinas Kominfo kota Lubuklinggau berdasarkan hasil analisa maka didapatkan permasalahan yang ada terletak pada tingkat keamanan server aplikasi SINANAN yang belum optimal, dimana saat ini belum ada penerapan sistem keamanan pada server, sehingga memungkinkan terjadinya serangan pada server SINANAN tersebut, sedangkan fungsi dari aplikasi tersebut sangat dibutuhkan setiap saat karena seluruh Aparat Sipil Negara (ASN) Kota Lubuklinggau, membutuhkan aplikasi tersebut untuk pengurusan yang terkait dengan kepegawaian serta SDM dari ASN tersebut.

Ada beberapa alternatif solusi untuk mengatasi permasalahan keamanan server SINANAN yang kurang maksimal, salah satunya adalah penerapan metode IDS (Intrusion Detection System). IDS (Intrusion Detection System) dapat didefinisikan sebagai tool yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan computer[16][17]. Salah satu IDS yang popular adalah SNORT, penggunaan Snort dalam sistem deteksi serangan dapat membantu mengidentifikasi aktivitas yang mencurigakan atau potensial serangan siber[18][19], dan memanfaatkan media telegram sebagai media notifikasi jika terjadi serangan atau aktifitas jaringan yang mencurigakan, telegram akan mengirimkan notifikasi serangan tersebut kepada admininstrator jaringan yang bertanggung jawab terhadap keamanan dari aplikasi SINANAN tersebut.

Dari analisis kebutuhan sistem yang telah diuraikan diatas maka dibutuhkan sebuah sistem yang dapat mendeteksi serangan terhadap server SINANAN Pada Diskominfo Lubuklinggau, sistem yang dibangun berbasis Intrusion Detection System (IDS) menggunakan SNORT dengan notifikasi Telegram[20]. Snort adalah salah satu program NIDS (Network Intrussion Detection System) yang bekerja untuk mendeteksi aktifitas secara real time terhadap lalu lintas jaringan dan paket. Snort melakukan analisa protocol dan content yang sama dengan pola pola serangan yang sudah ada[21][22].



Gambar 2. Alur Intrution Detection System (IDS)

RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

2.4 Metode Pengujian Sistem

Pengujian dilakukan dengan menggunakan metode eksperimen yang dimaksudkan apakah sistem Snort dapat mendeteksi serangan Ping of Death dengan baik. Pengujian dilakukan dengan menggunakan Ping of Death yang akan dilakukan oleh komputer client.

Tabel 1. Pengujian Sistem

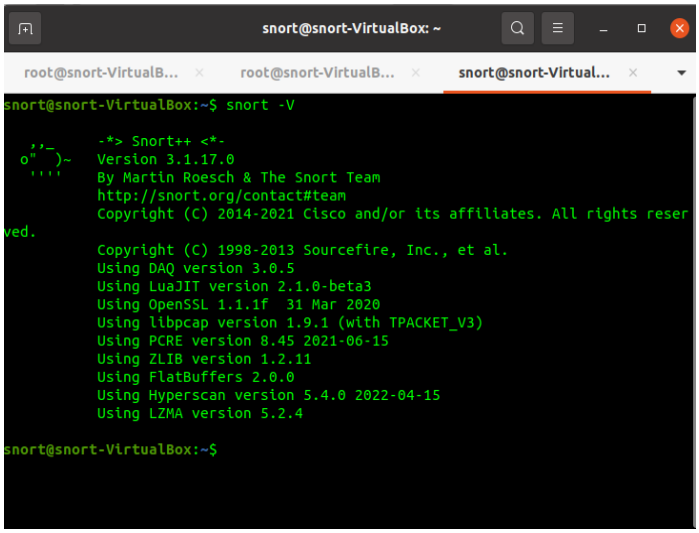
No	Komponen Pengujian	Proses Pengujian	Hasil Pengujian
1	Komputer server SINANAN	Kinerja Snort pada IDS.	Snort dapat mendeteksi serangan yang dilakukan client (Hacker).
2	Komputer Client (Hacker)	Melakukan ping of Death ke komputer server SINANAN.	Paket-paket data yang berisi serangan ping of death ke Server SINANAN
3	Handphone	Menerima notifikasi atau pemberitahuan saat terjadi serangan pada server	Telegram dapat mengirimkan notifikasi serangan kepada administrator jaringan

3. HASIL DAN PEMBAHASAN

Dari hasil dari penelitian selama kurang lebih enam bulan di Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Lubuklinggau, maka hasil yang diperoleh adalah penulis merancang sebuah sistem bot alert telegram berbasis snort untuk deteksi serangan ping of death. Sistem lama yang berjalan selama ini di tempat tersebut masih belum adanya sistem yang dapat mendeteksi serangan ping of death, sehingga rentan terkena serangan attacker, dalam hal ini sistem yang akan diterapkan sebagai langkah pengamanan dini terhadap server SINANAN di Diskominfotiksan Kota Lubuklinggau terhadap serangan menggunakan notifikasi telegram sehingga administrator jaringan lebih cepat mendapat alert (notifikasi) dari deteksi serangan tersebut.

3.1 Hasil Instalasi Snort

Hasil dari proses instalasi Snort pada server Ubuntu yang terdapat informasi tentang versi dari Snort yang di-install serta depedensi atau komponen aplikasi lainnya yang mendukung kinerja Snort.



Gambar 3. Hasil instalasi snort

Setiap komponen yang digunakan oleh Snort memiliki fungsi spesifik yang berkontribusi pada kinerja keseluruhan sistem deteksi dan pencegahan intrusi. Kombinasi dari komponen-komponen ini memungkinkan Snort untuk menangkap, menganalisis, dan merespons lalu lintas jaringan secara efisien dan efektif, serta untuk menulis aturan deteksi yang kompleks dan mendalam.

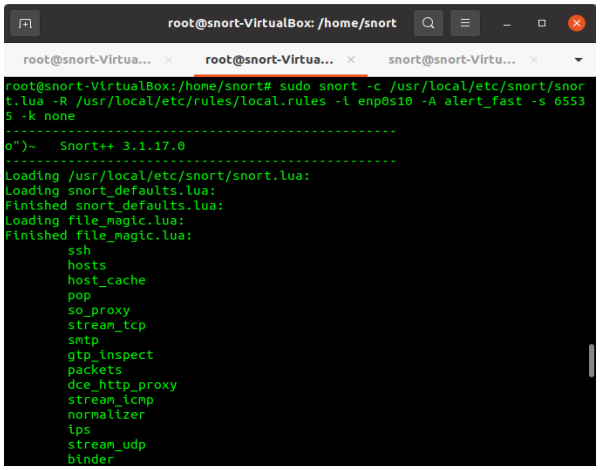
a. DAQ (Data Acquisition Library)
   Fungsi DAQ menyediakan abstraksi untuk metode pengambilan paket. Ini memungkinkan Snort untuk bekerja dengan berbagai sumber data jaringan, seperti pcap, afpacket, nfq, dan lainnya. DAQ memungkinkan fleksibilitas dalam cara Snort menangkap dan memproses paket jaringan, baik dalam mode inline maupun passive.
b. LuaJIT (Just-In-Time Compiler for Lua)
   Fungsi LuaJIT adalah kompilator JIT untuk bahasa pemrograman Lua, yang digunakan dalam Snort untuk memperluas fungsionalitasnya. Dengan LuaJIT, Snort dapat menjalankan skrip Lua dengan sangat cepat, memungkinkan pengguna untuk menulis aturan deteksi yang lebih kompleks dan kustomisasi yang lebih dalam.

RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

c. OpenSSL
Fungsi OpenSSL adalah toolkit yang menyediakan implementasi untuk protokol Secure Sockets Layer (SSL) dan Transport Layer Security (TLS). Dalam konteks Snort, OpenSSL digunakan untuk mengenkripsi komunikasi antara komponen Snort atau dengan server eksternal, serta untuk mendekripsi lalu lintas yang dienkripsi untuk analisis.
d. LibCap
Fungsi libpcap adalah library untuk menangkap jaringan paket, menyediakan antarmuka untuk mengakses data paket di jaringan. TPACKET_V3 adalah sebuah fitur dari kernel Linux yang mengoptimalkan kinerja pengambilan paket. Libpcap digunakan oleh Snort untuk menangkap dan menganalisis lalu lintas jaringan secara real-time.
e. PCRE (Perl Compatible Regular Expressions)
PCRE adalah library untuk memproses ekspresi reguler yang kompatibel dengan Perl. Dalam Snort, PCRE digunakan untuk menulis aturan deteksi yang mencakup pola pencarian kompleks dalam lalu lintas jaringan, seperti tanda tangan serangan atau pola lalu lintas berbahaya.
f. ZLIB
Mpresi dan mendekompresi data, terutama dalam konteks log dan data jaringan. Ini membantu mengurangi ukuran data yang perlu disimpan atau ditransmisikan.
g. FlatBuffers
FlatBuffers adalah library untuk serialisasi data yang dikembangkan oleh Google. Ini memungkinkan data untuk disimpan dan ditransmisikan dalam format biner yang sangat efisien. Dalam Snort, FlatBuffers digunakan untuk serialisasi dan deserialisasi data konfigurasi dan hasil deteksi.
h. Hyperscan
Hyperscan adalah library untuk pencocokan pola teks yang sangat cepat menggunakan mesin pencari ekspresi reguler. Dalam Snort, Hyperscan digunakan untuk mempercepat proses pencocokan pola dalam lalu lintas jaringan, memungkinkan deteksi ancaman yang lebih cepat dan efisien.
i. LZMA (Lempel-Ziv-Markov chain Algorithm)
LZMA adalah algoritma kompresi data yang digunakan untuk mengurangi ukuran data dengan efisiensi tinggi. Dalam Snort, LZMA dapat digunakan untuk mengkompresi data log dan data lainnya untuk menghemat ruang penyimpanan.

3.2 Hasil Start Snort

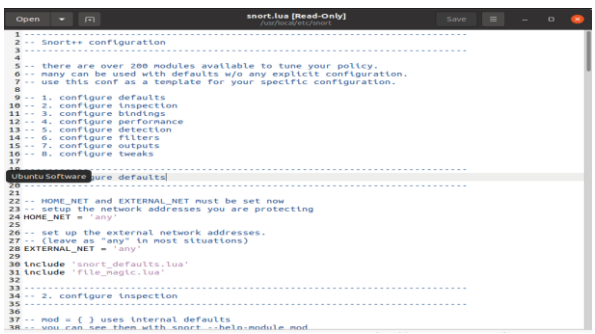
Untuk tahap pertama pengujian dari instalasi Snort adalah memulai Snort, apakah snort dapat berjalan pada server Ubuntu.



Gambar 4. Pengujian Hasil Instalasi

3.2.1 Hasil Konfigurasi Snort

Setelah berhasil dijalankan maka Snort harus di konfigurasi dahulu agar dapat mengamankan server.

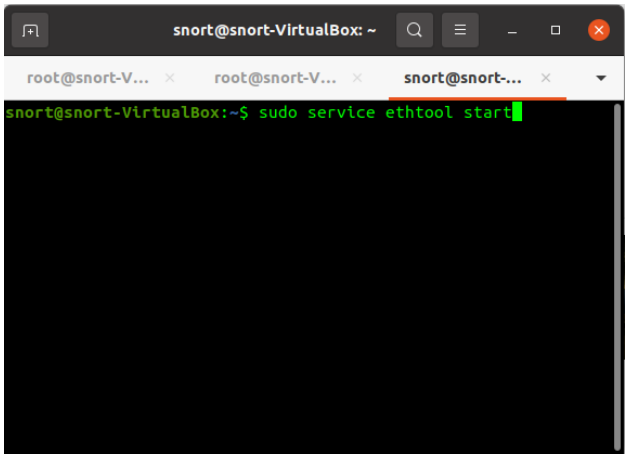


Gambar 5. Hasil Konfigurasi Snort

RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

3.2.1 Hasil Aktifasi Perangkat

Setelah selesai melakukan konfigurasi snort berhasil, maka tahap selanjutnya adalah mengakaktifasi perangkat Ethernet.



Gambar 6. Hasil Aktifasi Perangkat Ethernet

3.2.3 Hasil Konfigurasi Rules Snort

Rules Snort adalah aturan yang dirancang untuk mendeteksi serangan "Ping of Death". Ping of Death adalah serangan yang menggunakan paket ICMP (ping) dengan ukuran yang sangat besar untuk mencoba dan menyebabkan sistem target crash atau mengalami perilaku tidak normal., untuk itu perlu dilakukan konfigurasi pada rules snort.

Gambar 7. Hasil Konfigurasi Rules Snort

Gambar 7 menunjukan bahwa aturan snort didalam mendeteksi serangan pada sistem yang dilindungi oleh snort, penjelasannya sebagai berikut.

a. Alert: Tindakan yang akan diambil oleh Snort jika aturan ini cocok. Dalam kasus ini, Snort akan menghasilkan peringatan.
b. Icmp: Protokol yang dipantau oleh aturan ini, dalam hal ini adalah ICM
c. Any any: Bagian pertama any mewakili alamat IP sumber, dan bagian kedua any mewakili port sumber. Karena ini adalah protokol ICMP, port tidak relevan, sehingga any digunakan.P (Internet Control Message Protocol).
d. ->: Menunjukkan arah lalu lintas jaringan dari sumber ke tujuan.
e. Any any: Bagian pertama any mewakili alamat IP tujuan, dan bagian kedua any mewakili port tujuan.
f. Msg:"Snort Mendeteksi Serangan Ping of Death ": Pesan yang akan ditampilkan ketika aturan ini cocok. Pesan ini memberikan deskripsi singkat tentang apa yang terdeteksi.
g. Sid:10000001: Snort ID (SID) adalah pengidentifikasi unik untuk aturan ini. SID harus unik untuk setiap aturan dan digunakan untuk mengelola aturan.
h. Metadata: Metadata menyediakan informasi tambahan tentang aturan. Dalam hal ini, menunjukkan bahwa aturan ini adalah bagian dari kebijakan keamanan (security policy) untuk sistem pencegahan intrusi (IPS).

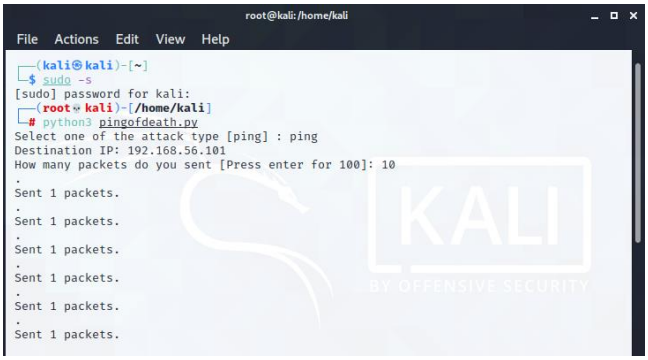
3.3 Pengujian Sistem

Pengujian sistem bot alert telegram sebagai notifikasi serangan ping of death pada server SINANAN berbasis Snort dilakukan menggunakan dua buah sistem operasi, satu sistem operasi Ubuntu Server sebagai server menggunakan sistem operasi Linux Ubuntu, dan sistem operasi Kali Linux lainnya sebagai penyerang (attacker), dan telegram sebagai penerima notifikasi serangan.

3.3.1 Pengujian Serangan

Proses penyerangan kepada server (Ubuntu) menggunakan sistem operasi Kali Linux, dengan memanfaatkan script serangan ping of death.

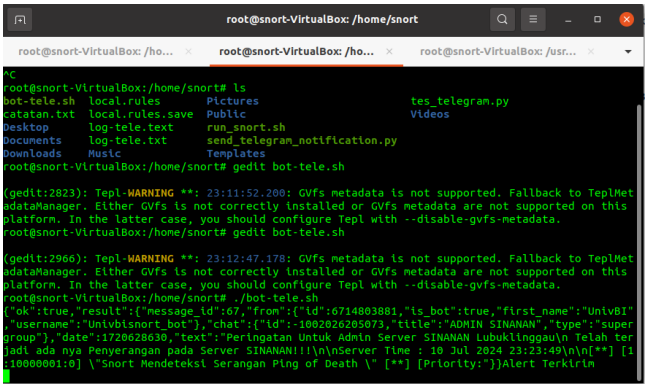
RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168



Gambar 8. Proses Serangan Ping of Death

3.3.2 Pengujian Mendeteksi Serangan

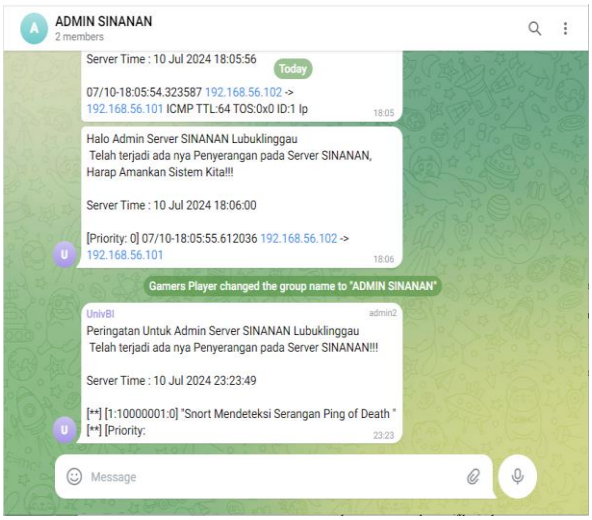
Proses pendeteksian serangan ping flooding oleh snort pada server Ubuntu dapat ditampilkan secara real time.



Gambar 9. Pengujian Serangan Ping of Death

3.3.3 Pengujian Notifikasi Serangan

Hasil pengujian menggunakan telegram dalam mendapatkan notifikasi dari deteksi serangan yang telah dilakukan oleh attacker pada server ubuntu, setiap kali ada serangan maka telegram dari administrator jaringan menerima notifikasi.



Gambar 10. Hasil Notifikasi Serangan dengan Telegram

3.4 Pembahasan

3.4.1 Proses Penyerangan

Proses penyerangan terhadap server yang menjalankan sistem operasi Ubuntu dilakukan menggunakan sistem operasi Kali Linux. Dalam proses penyerangan ini, script serangan "Ping of Death" digunakan untuk mengeksploitasi kelemahan dalam penanganan paket ICMP besar oleh server target. Dalam mengeksekusi serangan penyerang menjalankan terminal pada Kali Linux dan mengeksekusi script python, serangan tersebut mengirimkan paket ICMP dengan ukuran maksimum ke alamat IP target, disertai flag flood (-f) untuk mengirim paket dalam jumlah besar dan berkelanjutan.

ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

3.4.2 Proses Mendeteksi Serangan

Proses penyerangan terhadap server yang menjalankan sistem operasi Ubuntu dilakukan menggunakan sistem operasi Kali Linux. Dalam proses penyerangan ini ini, script serangan "Ping of Death" digunakan untuk mengeksploitasi kelemahan dalam penanganan paket ICMP besar oleh server target. Dalam mengeksekusi serangan penyerang menjalankan terminal pada Kali Linux dan mengeksekusi script python, serangan tersebut mengirimkan paket ICMP dengan ukuran maksimum ke alamat IP target, disertai flag flood (-f) untuk mengirim paket dalam jumlah besar dan berkelanjutan.

3.4.3 Proses Pengiriman Notifikasi Telegram

Proses pengiriman notifikasi adalah hasil Integrasi Snort dengan Telegram yang memungkinkan notifikasi serangan dikirimkan secara otomatis kepada administrator jaringan. Setiap kali snort mendeteksi terjadinya serangan, maka bot telegram akan mengirimkan notifikasi bahwa telah terjadi dugaan serangan pada server target.

4. KESIMPULAN

Berdasarkan hasil analisis, perancangan, dan evaluasi terhadap sistem bot alert Telegram berbasis Snort untuk mendeteksi serangan ping of death pada server SINANAN di Lubuklinggau, dapat disimpulkan bahwa sistem ini mampu mendeteksi serangan ping of death dari pihak yang tidak bertanggung jawab. Sistem ini mempermudah administrator jaringan dalam memantau serta mengamankan server melalui notifikasi real-time yang dikirimkan via Telegram, memungkinkan respons yang lebih cepat dan efisien terhadap ancaman keamanan. Hal ini membantu mengurangi potensi kerusakan yang lebih besar pada server SINANAN. Penelitian ini diharapkan dapat menjadi landasan untuk pengembangan lebih lanjut dalam meningkatkan keamanan server SINANAN. Salah satu saran yang diajukan adalah menambahkan fitur keamanan lainnya untuk melindungi server dari serangan siber yang lebih kompleks di masa mendatang, memastikan sistem keamanan dapat tetap efektif dan relevan. Penelitian ini memiliki batasan yaitu, sistem ini hanya diterapkan pada server SINANAN Kota Lubuklinggau, serangan yang dideteksi adalah serangan Denial of Service (DoS) dengan jenis ping of death, Intrusion Detection System (IDS) yang digunakan berbasis Snort, protokol yang digunakan adalah ICMP, dan pengujian sistem dilakukan dengan metode pengujian fungsional menggunakan server Ubuntu dan Kali Linux. Dengan adanya batasan ini, penelitian difokuskan pada ruang lingkup tertentu, namun hasilnya dapat dikembangkan untuk aplikasi yang lebih luas dalam sistem keamanan jaringan di masa depan.

REFERENCES

[1] P. Zuriati Ardila Safitri1, Elin Haerani, Rometdo Muzawi, Muhammad Affandes, “Intrusion Detection System (IDS) Pada Snort Dengan Bot Telegram Sebagai Sistem Notifikasi Terhadap Serangan Syn Flood dan Ping Of Death,” SATIN - Sains dan Teknol. Inf., vol. 10, no. 1, pp. 157–168, 2024, doi: 10.33372/stn.v9i2.1000..

[2] M. R. Ramadhan et al., “Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikasi Dengan Menggunakan Snort,” BHATARA J. Multidisiplin, vol. 1, no. 1, pp. 31–40, 2024, [Online]. Available: https://doi.org/.....IJCCS

[3] S. Khadafi, B. D. Meilani, and S. Arifin, “Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System),” J. IPTEK, vol. 21, no. 2, p. 67, 2017, doi: 10.31284/j.iptek.2017.v21i2.207.

[4] Z. Dwi Alfaeni, N. Fahriani, J. Raya Sutorejo No, D. Sutorejo, K. Mulyorejo, and J. Timur, “Deteksi Serangan Ddos Pada Jaringan Rt/Rw-Net Desa Ketanen Dengan Metode Intrusion Detection System (IDS) Menggunakan Snort,” Semin. Nas. Teknol. Inf. Ilmu Komput., vol. 2, no. 1, pp. 28–34, 2023.

[5] 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.

[6] A. Fergina, S. Alif, N. Ikhsan, and Z. Alamsyah, “Penggunaan Snort Sebagai Sistem Pendeteksi Serangan Pada Jaringan Menggunakan Notifikasi Telegram (Kasus Dinas Komunikasi Informatika Dan Persandian Kabupaten Sukabumi),” vol. 5, no. 3, pp. 901–912, 2024.

[7] I. P. G. A. Sudiatmika, I. P. Y. A. Ariwanta, and I. G. A. S. Melati, “Mengoptimalkan Keamanan Jaringan Komputer Menggunakan Snort dan Telegram Bot yang Terintegrasi dengan Mikrotik,” J. Comput. Syst. Informatics, vol. 3, no. 4, pp. 247–256, 2022, doi: 10.47065/josyc.v3i4.2037.

[8] Sutarti, A. P. Pancaro, and F. I. Saputra, “Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal,” J. PROSISKO, vol. 5, no. 1, pp. 1–8, 2018.

[9] B. Wijaya and A. Pratama, “Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort,” J. Sisfokom (Sistem Inf. dan Komputer), vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[10] G. Yandiputra Sunardi, A. Kania Ningsih, and S. Anggoro Universitas Jenderal Achmad Yani, “Sistem Monitoring Serangan Jaringan Menggunakan Intrusion Detection System (Ids) Dengan Notifikasi Telegram,” J. Ilm. Sain dan Teknol., vol. 2, no. 3, pp. 218–238, 2024, [Online]. Available: https://github.com/gperftools/gperftools/releases/download/gperftools-

[11] B. Sudradjat, “Sistem Pendeteksian dan Pencegahan Penyusup Pada Jaringan Komputer Dengan Menggunakan Snort dan Firewall,” JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Res., vol. 1, no. 1, pp. 10–24, 2017.

[12] 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.

[13] M. A. S. Arifin, “RANCANG BANGUN PROTOTYPE ROBOT LENGAN MENGGUNAKAN FLEX SENSOR DAN ACCELEROMETER SENSOR PADA LAB MIKROKONTROLER STMIK MUSIRAWAS,” vol. 9, pp. 255–261, 2017.

[14] S. Esabella and Y. Bella Fitriana, “KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Jaringan Menggunakan

ISSN 2745-7966 (Media Online)
Vol 5, No 1, September 2024 | Hal 49−57
https://djournals.com/resolusi
DOI: 10.30865/resolusi.v5i1.2168

Metode Security Policy Development Life Cycle (SPDLC)," Media Online, vol. 4, no. 1, pp. 634–641, 2023, doi: 10.30865/klik.v4i1.1157.

[15] M. Mukmin, P. Purnawansyah, and M. Hasnawi, "Notifikasi Bot Telegram Untuk Monitoring Jaringan Pada Kementrian Kelautan Dan Perikanan Untia," Bul. Sist. Inf. dan Teknol. Islam, vol. 3, no. 2, pp. 127–133, 2022, doi: 10.33096/busiti.v3i2.1162.

[16] D. Yuliandari, W. Walim, B. K. Raja, R. Ningsih, and A. J. Wahidin, "Simulasi Penerapan Sistem Monitoring Jaringan Snort NIDS Pada Web Server Menggunakan Metode SPDLC," J. Infortech, vol. 5, no. 2, pp. 133–138, 2023, doi: 10.31294/infortech.v5i2.17338.

[17] F. Nuraeni and I. Nurfajri, "Notifikasi Network Intrusion Detection System Menggunakan Media Aplikasi Telegram (Studi Kasus: Kantor Imigrasi Tasikmalaya)," J. Sist. Inf. dan Teknol. Inf. STMIK Dipanegara, vol. 6, no. 1, pp. 1–5, 2017, [Online]. Available: www.snort.org.

[18] R. K. Abdullah, M. T. Fudhail, S. Mujahidin, P. Studi, I. Jurusan, and T. Informasi, "Penggunaan Snort dan Fail2ban sebagai IDS untuk Mengatasi Brute Force Attack dengan Notifikasi Telegram : Studi Kasus pada Institusi XYZ The use of Snort and Fail2ban as IDS to overcome Brute Force Attack with Telegram notification : Case study at XYZ Institute," vol. 12, no. 3, pp. 530–542, 2024, doi: 10.26418/justin.v12i3.79617.

[19] E. Risyad, M. Data, and E. S. Pramukantoro, "Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood," J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 9, pp. 2615–2624, 2018.

[20] T. Purnama, Y. Muhyidin, and D. Singasatia, "Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi," J. Teknol. Inf. Dan Komun., vol. 14, no. 2, pp. 358–369, 2023, doi: 10.51903/jtikp.v14i2.726.

[21] A. Syaimi, P. Utami, L. Lidyawati, and Z. Ramadhan, "Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd," J. Reka Elkomika ©TeknikElektro | Itenas J. Online Inst. Teknol. Nas. J. Reka Elkomika, vol. 1, no. 4, pp. 2337–439, 2013.

[22] A. Muhaimi, I. P. Hariyadi, and A. Juliansyah, "Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram," J. Bumigora Inf. Technol., vol. 1, no. 2, pp. 167–176, 2019, doi: 10.30812/bite.v1i2.611.