Jurnal Nasional Teknologi Komputer
Vol.2; No: 3; Juli 2022
Website: publikasi.hawari.id/index.php/jnastek
E-ISSN: 2808-4845; P-ISSN: 2808-7801

Makalah Penelitian

PEMANFAATAN KERANGKA KERJA INVESTIGASI FORENSIK JARINGAN UNTUK IDENTIFIKASI SERANGAN JARINGAN MENGGUNAKAN SISTEM DETEKSI INTRUSI (IDS)

Abdul Khaliq[1], Sri Novida Sari[2]

[1]Sistem Komputer, Fakultas Ilmu Komputer, Universitas Pembangunan Panca Budi
[2]Teknik Informatika, Fakultas sains dan teknologi, Institut Teknologi dan Bisnis Indonesia
[1]abdulkhaliq@pancabudi.ac.id*, [2]srinovidasari@gmail.com

Corresponding Author: Abdul Khaliq

ABSTRACT

One of the media to secure computers is to apply Intrusion Detection System (IDS) technology. IDS is an early detection system in the event of a computer network attack. The IDS will alert the computer network administrator in the event of a computer network attack. IDS also records all attempts and activities aimed at disrupting computer networks and other computer network attacks. The purpose of this study is to implement IDS on network systems and analyze IDS logs to determine the types and types of computer network attacks. Logs on the IDS will be analyzed in depth to be used as an effort to improve computer network security. The research method that will be used is applied research. The research was carried out using the Network Forensic Investigation Framework proposed by Pilli, Joshi and Niyogi. The stages of the Network Forensic Investigation Framework are used to perform network simulations, analysis and investigations to determine the types of computer network attacks. The results show that the Network Forensic Investigation Framework facilitates the investigation process when a network attack occurs. The Network Forensic Investigation Framework is effectively used when the computer network has network security support applications such as IDS or others. IDS is effective in detecting network scanning activities and DOS attacks. IDS provides alerts to administrators because there are activities that violate the rules on the IDS.

Keywords: *DOS Attacks, Network Attack, Network Scanning, Network Forensic Investigation Framework*

ABSTRAK

Salah satu media untuk mengamankan komputer adalah dengan menerapkan teknologi Intrusion Detection System (IDS). IDS adalah sistem deteksi dini jika terjadi serangan jaringan komputer. IDS akan memperingatkan administrator jaringan komputer jika terjadi serangan jaringan komputer. IDS juga mencatat semua upaya dan aktivitas yang bertujuan mengganggu jaringan komputer dan serangan jaringan komputer lainnya. Tujuan dari penelitian ini adalah untuk mengimplementasikan IDS pada sistem jaringan dan menganalisis log IDS untuk menentukan jenis dan jenis serangan jaringan komputer. Log pada IDS akan dianalisis secara mendalam untuk digunakan sebagai upaya meningkatkan keamanan jaringan komputer. Metode penelitian yang akan digunakan adalah penelitian terapan. Penelitian dilakukan dengan menggunakan Network Forensic Investigation Framework yang diusulkan oleh Pilli, Joshi dan Niyogi. Tahapan Kerangka Kerja Investigasi Forensik Jaringan digunakan untuk melakukan simulasi jaringan, analisis dan investigasi untuk menentukan jenis serangan jaringan komputer. Hasil penelitian menunjukkan bahwa Network Forensic Investigation Framework memfasilitasi proses investigasi ketika terjadi serangan jaringan. Kerangka kerja investigasi forensik jaringan secara efektif digunakan ketika jaringan komputer memiliki aplikasi dukungan keamanan jaringan seperti IDS atau lainnya. IDS efektif dalam mendeteksi aktivitas pemindaian jaringan dan serangan DOS. IDS memberikan peringatan kepada administrator karena ada aktivitas yang melanggar aturan di IDS.

Kata Kunci: *Serangan DOS, Serangan Jaringan, Pemindaian Jaringan, Kerangka Kerja Investigasi Forensik Jaringan*

1. Pendahuluan

Akses internet merupakan prasyarat penting di era digital saat ini. Revolusi industri 4.0 mengamanatkan bahwa setiap orang terus-menerus terhubung ke internet untuk komunikasi. Institusi dan bisnis memasukkan internet ke dalam infrastruktur mereka untuk meningkatkan efisiensi karyawan dan bisnis. Kadang-kadang, pihak-pihak tertentu mengeksploitasi

popularitas Internet untuk meluncurkan serangan pada jaringan komputer. Di era digital ini, serangan terhadap jaringan komputer telah berkembang secara dramatis. Sejak 1 Januari 2020 hingga 12 April 2020, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Kripto Nasional (BSSN) mendokumentasikan 88.414.296 serangan siber di Indonesia. Pada Januari, tercatat 25.224.811 serangan, diikuti oleh 29.188 pada Februari, 645 pada Maret. Kemudian, ada 26.423.989 serangan pada Maret dan 7.576.851 serangan per 12 April 2020. (Iskandar, 2020). Serangan peretas tidak terbatas pada melumpuhkan jaringan komputer perusahaan. Selain itu, mereka mencoba mencuri data dari server.

Administrator jaringan komputer memiliki fungsi dan kewajiban penting di dalam suatu organisasi atau institusi. Administrator jaringan bertanggung jawab atas desain, perencanaan, operasi, dan keamanan jaringan, server, sakelar, jaringan Internet, dan semua komunikasi data organisasi. Perlindungan infrastruktur jaringan komputer dan data perusahaan dari serangan jaringan komputer adalah masalah yang sulit bagi manajer jaringan komputer. Serangan jaringan komputer atau serangan jaringan adalah upaya untuk mendapatkan akses tidak sah ke jaringan perusahaan untuk mencuri data atau melakukan tindakan destruktif lainnya. Intrusi adalah upaya yang tidak sah dan melanggar hukum untuk mengakses, memodifikasi, atau mengendalikan sistem/jaringan informasi dalam upaya untuk membuatnya tidak dapat diandalkan atau tidak dapat dioperasikan (Kumar, 2017). Ada banyak implementasi keamanan jaringan, dimulai dengan sistem AAA (Otentikasi, Otorisasi, dan Akuntansi), Firewall, Filter Perutean, Kontrol Akses, Sistem Pencegahan Intrusi, Sistem Deteksi Intrusi, dan Honeypots (Alsyaibani et al., 2021).

Administrator jaringan komputer dapat membangun Intrusion Detection System (IDS) untuk mengidentifikasi ancaman jaringan (Lazzez, 2013). IDS akan menawarkan manajer jaringan dengan pemberitahuan (peringatan) jika terjadi serangan atau gangguan jaringan. IDS saat ini mengandalkan deteksi berbasis tanda tangan atau model deteksi berbasis anomali, membuat metodologi deteksi mereka jauh dari sempurna jika dibandingkan dengan anomali yang berbeda dan teknologi baru yang digunakan oleh penyerang (Chowdhury et al., 2017).

Log yang direkam oleh IDS dapat dianalisis oleh administrator jaringan. Temuan analisis log IDS dapat digunakan untuk mengidentifikasi jenis serangan jaringan komputer yang ditujukan pada jaringan komputer, memungkinkan administrator jaringan untuk melakukan perbaikan, mengatur ulang jaringan, dan menyebarkan aplikasi tertentu untuk meningkatkan keamanan jaringan komputer yang dikelola.

Ada banyak penelitian tentang Sistem Deteksi Intrusi. Studi Khaerani dan Handoko (2015) berjudul "Implementasi dan Analisis Penambangan Data untuk Klasifikasi Serangan terhadap Sistem Deteksi Intrusi (IDS) Menggunakan Algoritma C4.5" memanfaatkan data dari tahun 1999. Pada saat itu, penggunaan Internet tidak seluas saat ini, dan serangan jaringan terhadap PC terbatas. Selain itu, Muhammad (2016) melakukan penelitian di mana ia secara eksplisit mengevaluasi data IDS menggunakan jaringan saraf untuk mengidentifikasi serangan DDOS. Sayangnya, penelitian ini terutama berfokus pada serangan jaringan DDOS, dan juga memprediksi kemungkinan serangan ini, sehingga sulit untuk disebarkan dan tidak mampu mengidentifikasi jenis serangan jaringan lainnya. Purba &Efendi (2021) juga melakukan penelitian dengan penekanan pada serangan DDOS yang mirip dengan mereka sendiri. Dalam penelitian lebih lanjut yang dilakukan oleh Suhartono dan Patta (2017), peneliti membatasi ruang lingkup serangan ke dua port jaringan, yaitu SSH dan FTP, sehingga membuat penelitian ini lebih menarik.

Penelitian ini berfokus pada implementasi Network Forensic Investigation Framework dengan ide-ide Snort IDS untuk mendeteksi berbagai macam serangan jaringan. Subjek ini juga menggabungkan unsur-unsur keamanan jaringan komputer dan forensik digital. Penelitian ini tidak dimaksudkan untuk menguji IDS dengan serangan tertentu; sebaliknya, ini berfokus pada

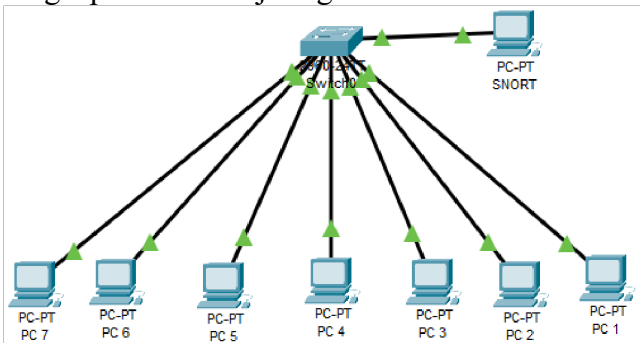
contoh penggunaan IDS dan bagaimana melakukan penyelidikan serangan jaringan menggunakan Kerangka Kerja Investigasi Forensik Jaringan dengan sukses dan mudah.

2. Metode Penelitian

Penelitian ini menggunakan metodologi penelitian terapan. Menurut Irina (2017), penelitian terapan dilakukan dengan mempertimbangkan realitas praktis dari penerapan dan pengembangan pengetahuan yang diberikan oleh penelitian dasar. Tujuan dari penelitian terapan adalah untuk menemukan solusi untuk tantangan tertentu. Tujuan utamanya adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia, baik secara individu maupun kolektif, atau untuk tujuan industri atau politik, dan bukan semata-mata untuk wawasan ilmiah. Penelitian ini akan menggunakan Kerangka Kerja Investigasi Forensik Jaringan sembilan tahap yang disediakan oleh Pilli et al. (2010).

2.1. Persiapan dan Otorisasi

Seperti yang ditunjukkan pada Gambar 1, kita sekarang akan membangun sistem jaringan yang terdiri dari 7 PC klien, 1 switch, dan 1 PC dengan Snort IDS diinstal. Kerangka kerja ini juga memerlukan otorisasi lengkap dan sistem jaringan serta akses Snort IDS.



Gambar 1. Desain Topologi Jaringan Simulasi

2.2. Deteksi dan Kejahatan/Insiden

Setelah jaringan dan Snort IDS telah digunakan dan dikonfigurasi, banyak simulasi serangan jaringan akan dilakukan. Uji coba ini akan mencakup metode serangan jaringan langsung, seperti pemindaian jaringan dan serangan DOS. Aturan IDS untuk mendeteksi pemindaian jaringan dan serangan DOS akan diperkenalkan. IDS akan mengevaluasi aktivitas jaringan berdasarkan aturan yang disediakan dan memberikan peringatan (peringatan) kepada administrator jika ada aktivitas yang melanggar batasan.

2.3. Respons Insiden

Adanya peringatan (peringatan) dari Snort IDS mendorong implementasi respons insiden. Respons selanjutnya akan melibatkan perubahan dan modifikasi aturan Snort IDS. Beberapa modifikasi aturan digunakan untuk menentukan kemampuan dan kapasitas Snort IDS.

2.4. Kumpulan Jejak Jaringan

Melacak dan memvalidasi kesesuaian sumber serangan, jenis serangan, dan peringatan Snort IDS setelah serangan pada jaringan komputer.

2.5. Pelestarian dan Perlindungan

Fase ini mencakup keamanan data yang menunjukkan serangan jaringan. Bukti ini diberikan oleh Snort IDS dalam bentuk log dan peringatan. Perlindungan ini diperlukan karena serangan

tertentu memungkinkan penghapusan jejak dan bukti.

2.6. Pemeriksaan
Pemeriksaan data digunakan untuk membedakan data aktivitas reguler dari data yang berkaitan dengan serangan jaringan komputer. Pemeriksaan ini juga digunakan untuk mengetahui keberadaan sumber data selain log IDS yang dapat membantu dalam prosedur analisis.

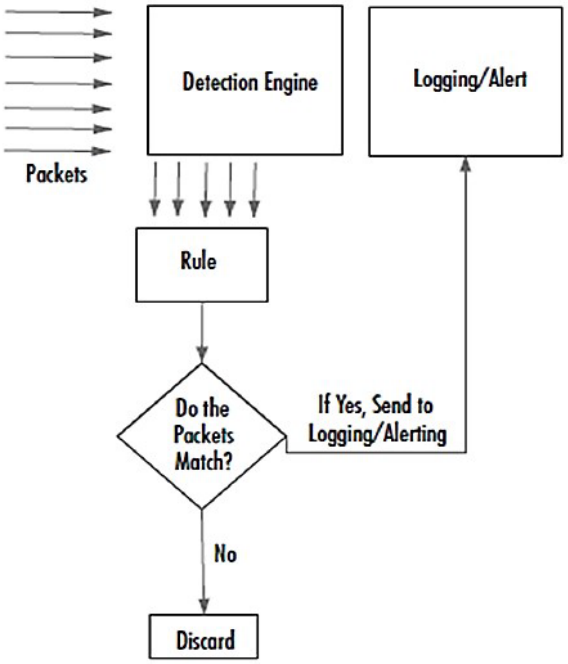
2.7. Analisis
Bukti yang diperoleh kemudian dievaluasi dengan menggunakan berbagai prosedur dan instrumen. Analisis ini menggunakan banyak karakteristik, termasuk jenis koneksi jaringan, sistem operasi, dan protokol jaringan.

2.8. Investigasi dan Atribusi
Hasil analisis kemudian diperiksa untuk menentukan komputer mana yang meluncurkan serangan, komputer siapa itu, bentuk serangan apa yang digunakan, dampak serangan pada sistem, dan bagaimana menanggapi serangan berikutnya.

2.9.Presentasi
Hasil penelitian akan membuat laporan dan penjelasan yang lebih sederhana untuk dipahami oleh semua pihak yang terlibat. Presentasi ini juga mencakup rekomendasi bermanfaat dan langkah-langkah korektif untuk meningkatkan keamanan jaringan.

3. HASIL DAN DISKUSI

IDS adalah aplikasi perangkat atau perangkat lunak yang memantau aliran data di jaringan komputer untuk aktivitas berbahaya atau pelanggaran kebijakan (Barracuda Networks, 2021). Ada beberapa jenis sistem deteksi intrusi, termasuk: a) Network Intrusion Detection Systems (NIDS), yang memeriksa aliran data jaringan komputer. b) Sistem Deteksi Intrusi Berbasis Host (HIDS), yang memantau file sistem operasi.
Intrusion Detection System (IDS) menggunakan pendekatan deteksi berbasis tanda tangan dan anomali (Alviana & Sumitra, 2018). Menurut Alviana dan Sumitra (2018), metode berbasis anomali mendeteksi serangan melalui pola lalu lintas jaringan yang tidak biasa, sedangkan metode berbasis tanda tangan mendeteksi serangan melalui pola atau paket data yang dibaca dan kemudian dibandingkan dengan data atau paket yang telah disimpan dalam database atau aturan yang ada.
Snort adalah sistem deteksi intrusi sumber terbuka (IDS) yang banyak digunakan yang mendeteksi intrusi atau lalu lintas jaringan yang tidak biasa (Paramitha et al., 2020). Snort adalah contoh program Sistem Deteksi Intrusi Berbasis Jaringan (Sandi &Arrofiq, 2018). Snort beroperasi mirip dengan TcpDump, tetapi dengan penekanan pada mengendus paket keamanan. Fitur utama Snort yang membedakannya dari TcpDump adalah payload inspection, di mana ia menganalisis payload rule list yang ditentukan (Dewi, 2017).
Menurut Singh dan Tomar (2015), Snort beroperasi dalam mode IDS sebagai mesin pendeteksi. Ketika sebuah paket melewati sakelar, mesin deteksi Snort akan mendeteksinya, dan kemudian, sebagai IDS, Snort akan mencocokkan paket dengan aturan yang dikonfigurasi. Ketika paket tidak sesuai dengan aturan (paket berisi materi serangan), itu disimpan dalam log Snort dan alarm dihasilkan. Namun, jika paket sesuai dengan aturan (paket tidak mengandung konten serangan), itu diabaikan dan langsung ditransmisikan.

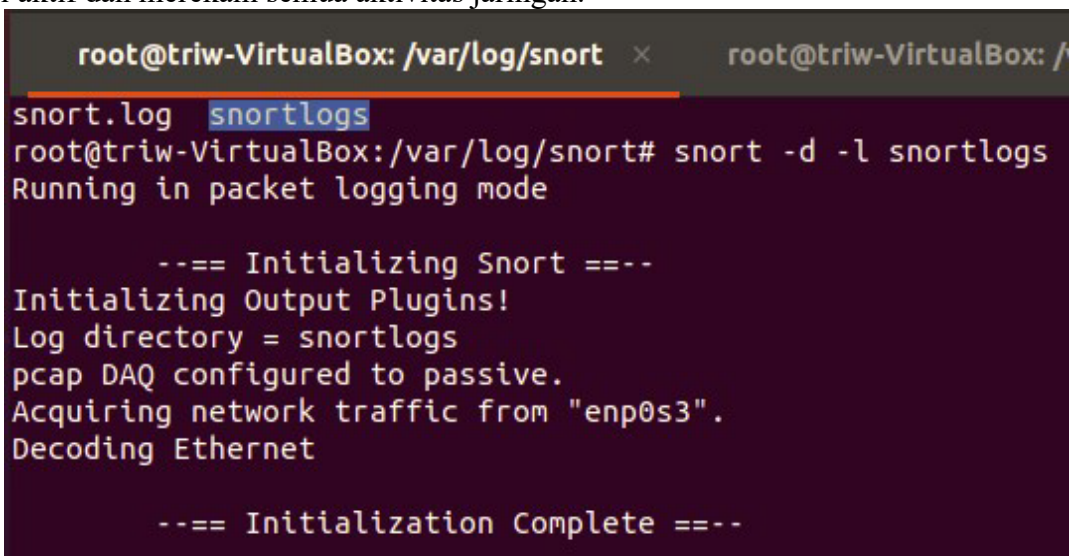


Gambar 2. Cara Kerja Mesin Pendeteksi Snort (Singh & Tomar, 2015)

Administrator jaringan dapat menggunakan data log IDS Snort ini untuk mengevaluasi kinerja sistem keamanan jaringan (Paramitha et al., 2020). Implementasi Kerangka Kerja Investigasi Forensik Jaringan yang dikembangkan oleh Pilli et al. (2010), yang terdiri dari sembilan (sembilan) langkah, dijelaskan di bawah ini.

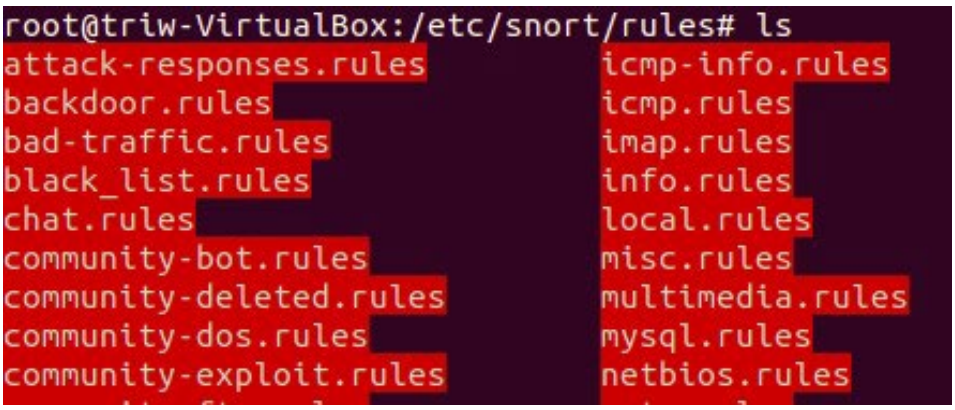
3.1. Persiapan dan Otorisasi

Jaringan komputer dilengkapi dengan banyak program keamanan, seperti firewall, perangkat lunak anti-virus, proxy, dan sistem deteksi intrusi (IDS). Administrator jaringan harus memiliki akses dan kontrol penuh atas jaringan komputer yang dikelola. Administrator juga memastikan bahwa aplikasi keamanan ini beroperasi. Gambar 3 menunjukkan bahwa IDS Snort berada di posisi aktif dan merekam semua aktivitas jaringan.



Gambar 3. Mengaktifkan Mode Logging di Snort

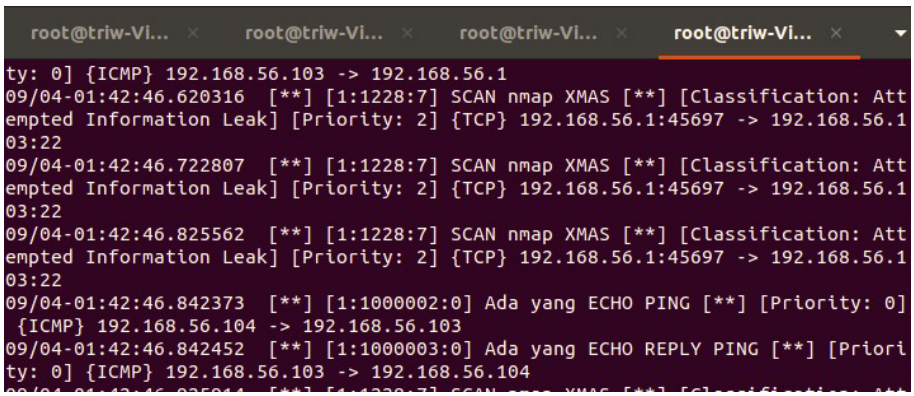
Snort IDS beroperasi berdasarkan aturan yang ditentukan administrator. Aturan ini akan berfungsi sebagai standar untuk operasi IDS, seperti menolak paket, meneruskan paket, dan mengeluarkan alarm. Seperti yang ditunjukkan pada Gambar 4, aturan ini dapat dibagi menjadi beberapa aturan.



Gambar 4. Konfigurasi Aturan di Snort

3.2. Deteksi dan Kejahatan/Insiden

IDS Snort akan mengidentifikasi berbagai serangan berdasarkan seperangkat aturan. Snort akan memberi administrator peringatan atau peringatan terhadap ancaman atau akses jaringan tertentu, seperti yang digambarkan pada Gambar 5. Dalam penyelidikan ini, PC 4 mencoba memindai dan menginventarisasi komputer server. Prosedur pemindaian dapat dideteksi oleh Snort IDS. Selain itu, PC 4 secara teratur mentransmisikan ping, yang mungkin menyarankan serangan DOS.



Gambar 5. Peringatan ditampilkan di Konsol Setelah Mendeteksi Serangan

3.3. Respons Insiden

Ketika administrator menerima peringatan atau alarm yang dikeluarkan oleh IDS. Banyak opsi berikutnya tersedia untuk administrator, seperti membatasi port, seperti yang diwakili pada Gambar 6, memblokir alamat IP, dan menonaktifkan protokol tertentu.

Gambar 6. Respon Yang Terdiri dari Penutupan Pelabuhan Tertentu

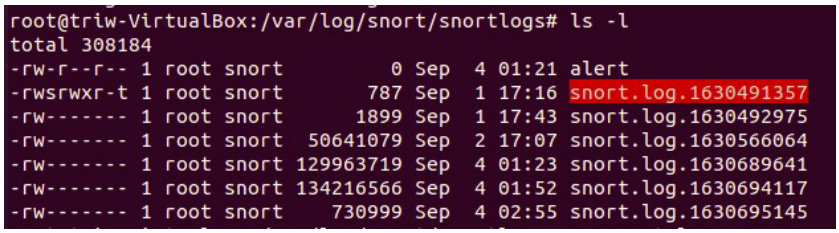
Administrator juga dapat mengoptimalkan keamanan jaringan dengan memodifikasi banyak

aturan, seperti yang ditunjukkan pada Gambar 7.

Gambar 7. Penyesuaian dan Perubahan Aturan Mendengus untuk Mengantisipasi Serangan Jaringan

3.4. Kumpulan Jejak Jaringan

Seperti yang ditunjukkan pada Gambar 8, setiap aktivitas jaringan akan direkam oleh ids pada log atau catatan.



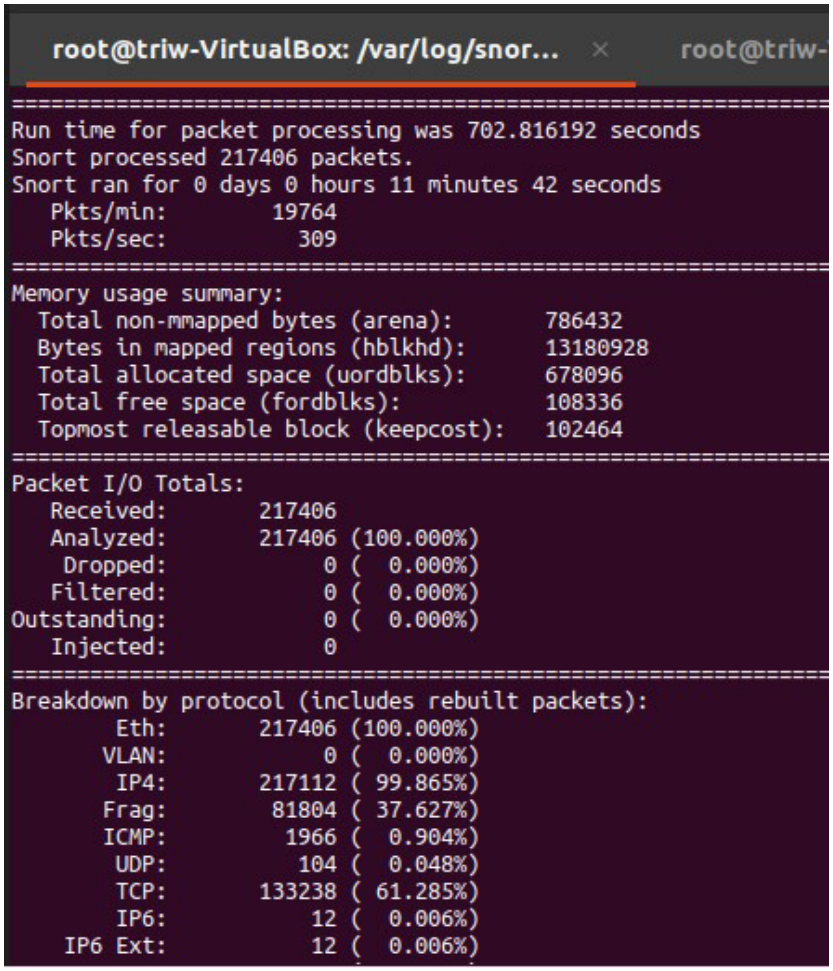
Gambar 8. Log aktivitas diperoleh melalui Snort Log

3.5. Pelestarian dan Perlindungan

Saat mengidentifikasi keberadaan serangan atau gangguan jaringan, tugas administrator selanjutnya adalah mengamankan log atau catatan yang direkam oleh IDS Snort, karena log atau catatan ini akan berisi informasi penting mengenai jenis serangan, sumber serangan, dan protokol yang ditargetkan.

3.6.Pemeriksaan

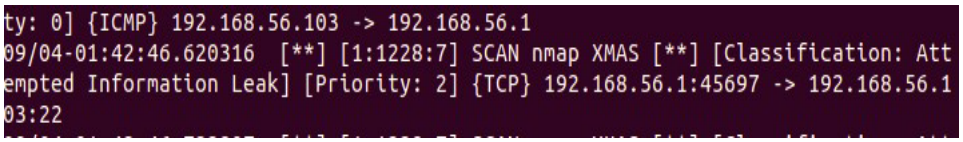
Setelah memperoleh catatan atau log DARI SNORT IDS, administrator jaringan melakukan pemeriksaan dan identifikasi aktivitas jaringan komputer. Seperti yang terlihat pada Gambar 9, log Snort IDS akan berisi informasi tentang aktivitas jaringan seperti ukuran paket dan protokol yang digunakan.



Gambar 9. Hasil untuk Rekaman Aktivitas Jaringan Snort

3.7. Analisis

Log memberi tahu administrator bahwa alamat IP penyerang, 192.168.56.103, adalah sumber pemindaian port pada server 192.168.56.1, seperti yang digambarkan pada Gambar 10.



Gambar 10. Tentukan Asal Usul Serangan Jaringan

3.8.Investigasi dan Atribusi

Administrator menentukan bahwa PC 4 192.168.56.103 telah mengirim paket 217406 selama 11 menit dan 42 detik. Administrator menentukan bahwa host dengan alamat IP 192.168.56.103 juga telah mengirimkan paket yang berisi 13180928 byte, atau sekitar 206 MB, yang dapat menjadi indikasi banjir paket atau serangan DOS. PC 4 juga disarankan untuk melakukan pencacahan berbasis pemindaian. Diduga bahwa PC 4 sedang mencari komputer server untuk kelemahan keamanan.

3.9.Presentasi

Langkah terakhir administrator dalam forensik digital adalah menyusun laporan tentang temuan investigasi sehingga temuan tersebut dapat dikomunikasikan kepada pimpinan dan ditindaklanjuti dengan perubahan keamanan jaringan.

4. KESIMPULAN

Studi ini menunjukkan bahwa Kerangka Kerja Investigasi Forensik Jaringan memfasilitasi proses investigasi serangan jaringan. Ketika jaringan komputer berisi program dukungan keamanan jaringan, seperti IDS atau yang lainnya, Kerangka Kerja Investigasi Forensik Jaringan dapat digunakan secara efisien. IDS mendeteksi pemindaian jaringan dan serangan DOS dengan presisi. IDS memberi tahu administrator ketika mendeteksi perilaku yang melanggar aturannya. Rekaman atau log IDS memudahkan prosedur investigasi, memungkinkan serangan jaringan dilacak kembali ke asal dan vektornya. Diharapkan bahwa penelitian di masa depan akan menggabungkan perangkat keamanan jaringan dengan kecerdasan buatan atau perangkat pembelajaran mesin. Untuk mendeteksi intrusi pornografi dan malware, penelitian yang mengintegrasikan aplikasi keamanan jaringan komputer dengan kecerdasan buatan atau pembelajaran mesin sangat signifikan.

REFERENSI

[1] Uğurlu, M., & Doğru, İ. A. (2019, September). Survei tentang sistem deteksi intrusi berbasis pembelajaran mendalam. Pada tahun 2019 4th International Conference on Computer Science and Engineering (UBMK) (hlm. 223-228). IEEE.

[2] Zhou, X., Liang, W., Li, W., Yan, K., Shimizu, S., Kevin, I., & Wang, K. (2021). Serangan musuh hierarkis terhadap sistem deteksi intrusi jaringan ioT berbasis jaringan saraf grafik. Jurnal Internet of Things IEEE.

[3] Kumar, P., Gupta, G. P., & Tripathi, R. (2021). Desain sistem deteksi intrusi berbasis anomali menggunakan komputasi kabut untuk jaringan IoT. Kontrol Otomatis dan Ilmu Komputer, 55(2), 137-147.

[4] Ghabban, F. M., Alfadli, I. M., Ameerbakhsh, O., AbuAli, A. N., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021, Juni). Analisis komparatif alat forensik jaringan dan proses forensik jaringan. Pada Tahun 2021 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (hlm. 78-83). IEEE.

[5] Barik, K., Das, S., Konar, K., Banik, B. C., & Banerjee, A. (2021). Menjelajahi persyaratan pengguna alat forensik jaringan. Proses Transisi Global, 2(2), 350-354.

[6] Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Kerangka kerja forensik jaringan: Tantangan survei dan penelitian. investigasi digital, 7(1-2), 14-27.

[7] IQBAL, M., HAMDANI, M. S. H., NABABAN, A. A., FOZILJONOVA, N., WASITO, I., BENTALEB, A., ... & FIRDAUS, A. (2022). NEURO NETWORK TECHNIQUES OF TELEMETRY MULTIVARIATE TIME SERIES PROCESSING AND THEIR APPLICATIONS IN INDUSTRY. Journal of Theoretical and Applied Information Technology, 100(09).

[8] Iqbal, M., Zarlis, M., Tulus, T., & Mawengkang, H. (2020, February). Model Pendekatan Metaheuristik Dalam Penyelesaian optimisasi Kombinatorial. In Seminar Nasional Teknologi Komputer & Sains (SAINTEKS) (Vol. 1, No. 1, pp. 92-97).

[9] Sangher, K. S., & Singh, A. (2019, April). Tinjauan sistematis–optimasi algoritma deteksi intrusi untuk analisis dan investigasi forensik jaringan. Pada Konferensi Internasional 2019 tentang Otomasi, Komputasi dan Manajemen Teknologi (ICACTM) (hlm. 132-136). IEEE.

******