ANALISIS KOMPARATIF UKURAN DAN INTENSITAS SERANGAN DDOS PADA UDPLAG, LDAP, DAN PORTMAP MENGGUNAKAN DATASET CIC-DDOS2019

Nabiel Ilyasa Pradana[1], Aditya Nur Wicaksono[2], Fahrul Islami Arsya Feri[3], Leli Nisfi Setiana[4]
Teknik Informatika, Universitas Islam Sultan Agung Semarang
Jl. Kaligawe Raya No.Km.4, Terboyo Kulon, Kec. Genuk,
Kota Semarang, Jawa Tengah 50112
e-mail: *[1]32602300046@std.unissula.ac.id , [2]widiyatminiarif@gmail.com,
[3]fahrulferi8@gmail.com, 4lelinisfi@unissula.ac.id

Abstrak

Distributed Denial of Service (DDoS) attacks have become a persistent threat to digital infrastructure, requiring efficient detection and mitigation strategies. This study presents a comparative analysis of three specific types of DDoS attacks: UDPLag, LDAP, and Portmap, using the CIC-DDoS2019 dataset from the Canadian Cyber Security Institute. The primary objective is to examine the patterns and impacts of each attack based on packet size distribution, temporal characteristics, and industry-level severity using CVE-style classification. The methodology includes descriptive statistics, visualizations (such as histograms, boxplots, time-based histograms, heatmaps, and pairplots), and t-SNE dimensionality reduction to observe data clustering among the attacks. The results show that LDAP attacks exhibit the largest packet size and volume, while Portmap has the highest risk label despite having a smaller data volume. UDPLag, although consisting of smaller packets, demonstrates moderate intensity and high frequency. These findings indicate that each type of attack behaves differently and carries distinct risk levels.The study concludes that integrating visual analytics with CVE-based references provides valuable insights for prioritizing DDoS mitigation strategies according to the type and behavior of the attack.

Keywords: *CIC-DDoS2019 dataset, Cybersecurity, DDoS attacks, Mitigation strategies, Risk assessment*

PENDAHULUAN

Di era digital, keamanan jaringan menjadi masalah penting. Ini terutama terkait dengan serangan *Distributed Denial of Service* (DDoS), yang meningkat dalam frekuensi dan kompleksitas. Serangan DDoS membanjiri layanan target dengan lalu lintas jaringan yang besar, mengganggu atau menghentikan layanan. Lebih dari 13 juta serangan DDoS tercatat di seluruh dunia pada tahun 2022, dengan serangan berbasis protokol dan multivektor yang meningkat (Netscout, 2023). Serangan ini sangat efektif karena dapat menyamar sebagai lalu lintas jaringan yang sah dan mengeksploitasi berbagai celah pada protokol seperti UDP, LDAP, dan RPC/Portmapper (Cloudflare, 2023). Untuk menghadapi tantangan tersebut, diperlukan pendekatan analitis berbasis data nyata guna mengenali pola dan dampak dari tiap jenis serangan. Dataset CIC-DDoS2019 yang dikembangkan oleh *Canadian Institute for Cybersecurity* menyediakan data lengkap serangan DDoS dalam berbagai bentuk, termasuk UDPLag, LDAP, dan Portmap, yang banyak digunakan dalam penelitian keamanan siber (Sharafaldin et al., 2019). Penelitian sebelumnya banyak berfokus pada deteksi serangan DDoS menggunakan algoritma pembelajaran mesin seperti Random Forest dan SVM. Namun, sebagian besar studi tersebut lebih menekankan pada aspek klasifikasi dan belum memberikan analisis mendalam terkait perbedaan karakteristik setiap jenis serangan (Vinayakumar et al., 2019). Selain itu, hanya sedikit studi yang mengaitkan serangan DDoS dengan sistem klasifikasi kerentanan industri seperti *Common Vulnerabilities and Exposures* (CVE), yang dapat memberikan konteks urgensi dan prioritas mitigasi (MITRE, 2024).

Penelitian ini bertujuan untuk melakukan analisis komparatif terhadap tiga jenis serangan DDoS—UDPLag, LDAP, dan Portmap—berdasarkan data CIC-DDoS2019. Penelitian ini menggunakan teknik visualisasi eksploratif dan statistik untuk menghitung perbedaan berdasarkan klasifikasi CVE untuk ukuran paket, waktu kejadian, jumlah data, dan tingkat urgensi. Perbedaan utama dari penelitian ini dengan penelitian sebelumnya adalah integrasi konteks praktis berbasis data CVE dan analisis dampak serangan secara visual, yang dapat meningkatkan strategi mitigasi berbasis risiko.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan metode eksplorasi data dan visualisasi statistik. Data yang digunakan dalam penelitian ini bersumber dari dataset CIC-DDoS2019 yang disediakan oleh Canadian Institute for Cybersecurity (Canadian Institute for Cybersecurity, 2019). Dataset ini berisi rekaman lalu lintas jaringan yang mencakup berbagai jenis serangan DDoS, namun dalam penelitian ini difokuskan pada tiga jenis serangan utama, yaitu UDPLag, LDAP, dan Portmap.

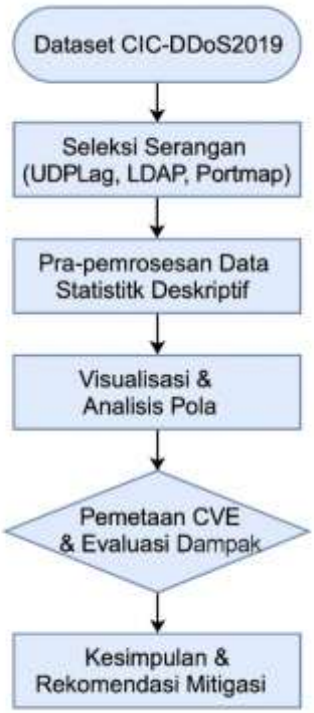
Rancangan Penelitian

Rancangan penelitian pada Gambar 1 terdiri dari enam tahap utama, yaitu:

1. **Pengumpulan Data**
   Mengambil subset data dari CIC-DDoS2019 yang relevan dengan jenis serangan UDPLag, LDAP, dan Portmap dalam format CSV. Dataset UDPLag memiliki 725.165 data, dataset LDAP memiliki 2.113.234 data, dan dataset Portmap memiliki 191.694 data.
2. **Pra-pemrosesan Data**
   Melakukan pembersihan data seperti menghapus data duplikat, serta mengidentifikasi kolom yang relevan untuk analisis seperti ukuran paket dan timestamp. Pada dataset ini, tidak dilakukan pengisian nilai kosong karena seluruh kolom yang digunakan untuk analisis tidak memiliki data hilang, sehingga langkah *fillna()* atau penggantian nilai kosong tidak diperlukan.
3. **Analisis Statistik Deskriptif**
   Menghitung nilai-nilai statistik seperti rata-rata, minimum, dan maksimum dari atribut utama (contoh: Total Packet Size) untuk masing-masing jenis serangan.
4. **Visualisasi Data**
   Menggunakan teknik visualisasi seperti histogram, boxplot, dan heatmap untuk mengevaluasi distribusi ukuran paket, intensitas waktu, dan hubungan antar atribut.
5. **Klasifikasi Tingkat Risiko Berdasarkan CVE**
   Masing-masing jenis serangan dikaitkan dengan entri *Common Vulnerabilities and Exposures* (CVE) untuk menentukan tingkat urgensi berdasarkan standar industri.
6. **Reduksi Dimensi dan Klasterisasi (Opsional)**
   Menggunakan metode t-SNE (t-distributed stochastic neighbor embedding) untuk memvisualisasikan pola distribusi data multidimensi ke dalam ruang 2D, sebagai bentuk identifikasi klaster pola serangan.

Kerangka Penelitian

Berikut adalah kerangka alur penelitian secara umum:



Gambar 1. *Flowchart* Metode Penelitian

Metode Analisis Data

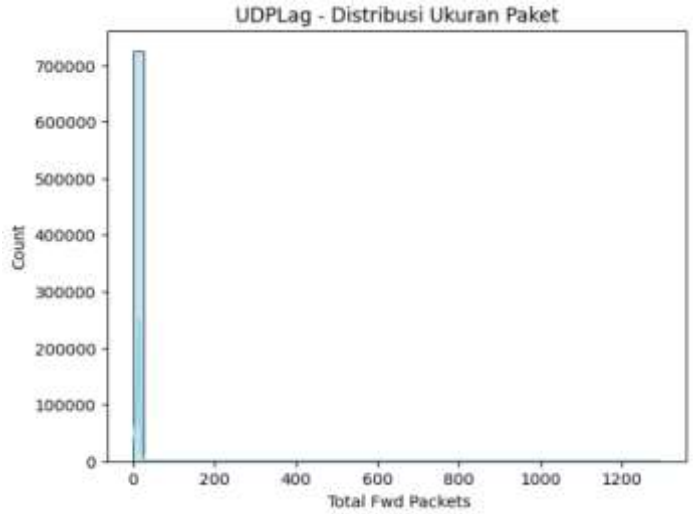
Data yang terkumpul dianalisis menggunakan pendekatan *content analysis* dan *thematic analysis*. *Content analysis* digunakan untuk menelaah struktur data teknis pada dataset CIC-DDoS2019, termasuk atribut seperti ukuran paket, durasi aliran, dan jumlah paket yang dikirim. Analisis ini dilakukan menggunakan bahasa pemrograman Python dengan bantuan pustaka seperti **Pandas** untuk manipulasi data dan **Seaborn/Matplotlib** untuk eksplorasi visual. Sementara itu, *thematic analysis* digunakan untuk mengelompokkan hasil temuan ke dalam tema-tema utama, seperti jenis serangan (UDPLag, LDAP, dan Portmap), pola distribusi waktu, intensitas serangan, dan tingkat risiko berdasarkan referensi dari *Common Vulnerabilities and Exposures* (CVE). Informasi CVE diperoleh melalui pencocokan manual dari sumber resmi https://cve.mitre.org, yang digunakan untuk menilai tingkat urgensi dan kerentanan masing-masing jenis serangan. Untuk memastikan keabsahan interpretasi karakteristik serangan dan mendukung saran mitigasi yang didasarkan pada bukti, triangulasi sumber memastikan validitas data dengan membandingkan hasil eksplorasi statistik, visualisasi grafik, dan referensi eksternal dari laporan industri keamanan jaringan dan dokumentasi CVE.

HASIL DAN PEMBAHASAN

Penelitian ini berhasil mengidentifikasi dan membandingkan karakteristik tiga jenis serangan DDoS, yaitu UDPLag, LDAP, dan Portmap, dengan menganalisis data dari CIC-DDoS2019. Hasil pengolahan data menunjukkan bahwa masing-masing jenis serangan memiliki pola dan dampak yang berbeda secara signifikan, baik dari segi ukuran paket, frekuensi, maupun tingkat urgensi berdasarkan CVE.

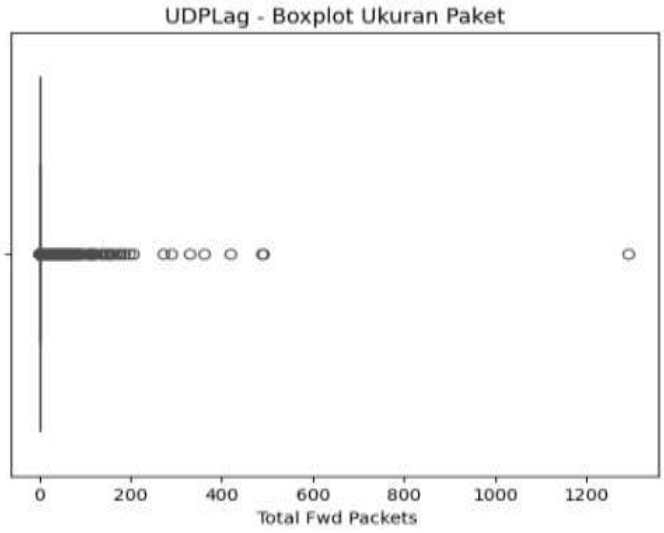
Distribusi Ukuran Paket dan Outlier

Analisis deskriptif menunjukkan bahwa serangan LDAP memiliki nilai maksimum ukuran paket tertinggi, yaitu mencapai 87.193 bytes, sementara Portmap mencapai 20.444 bytes dan UDPLag hanya 1.294 bytes. Rata-rata ukuran paket LDAP juga lebih tinggi dibanding dua jenis lainnya.



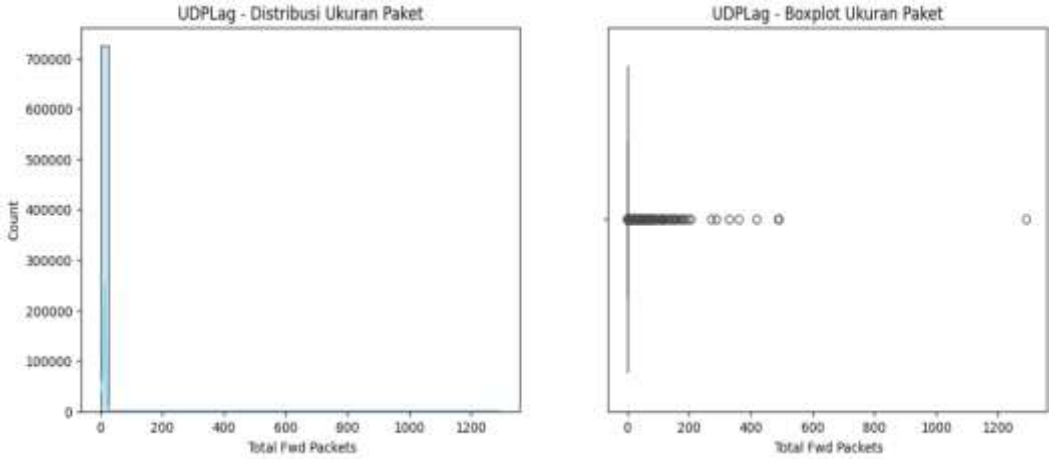
Gambar 2. Histogram ukuran paket serangan LDAP

Gambar 2 memperlihatkan distribusi ukuran paket serangan UDPLag yang cenderung terkonsentrasi pada jumlah paket kecil (di bawah 200 Total Fwd Packets) dengan frekuensi yang sangat tinggi, menunjukkan karakteristik serangan berupa pengiriman paket kecil secara berulang dalam jumlah besar



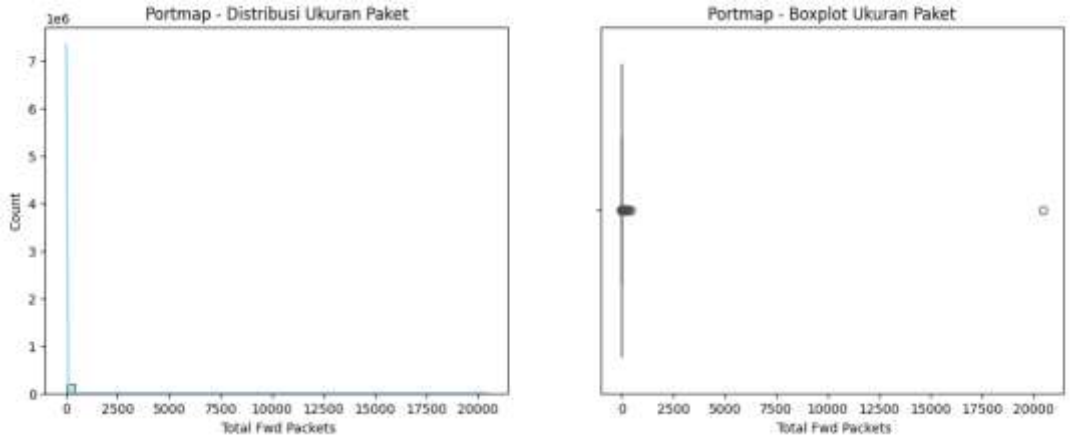
Gambar 3. Boxplot distribusi ukuran paket LDAP

Gambar 3 menunjukkan boxplot ukuran paket serangan UDPLag. Distribusi paket didominasi oleh nilai kecil yang rapat di sekitar median, namun terdapat sejumlah outlier dengan ukuran paket lebih besar hingga di atas 1200 Total Fwd Packets. Hal ini mengindikasikan bahwa sebagian kecil trafik memiliki ukuran paket yang jauh lebih besar dibandingkan mayoritas.



Gambar 4. Histogram dan boxplot ukuran paket UDPLag

Gambar 4 menunjukkan distribusi ukuran paket serangan UDPLag melalui histogram (kiri) dan boxplot (kanan). Histogram memperlihatkan mayoritas paket memiliki ukuran kecil dengan jumlah yang sangat besar, sedangkan boxplot mengonfirmasi adanya konsentrasi paket di sekitar nilai rendah dengan beberapa outlier yang berukuran lebih besar. Pola ini menunjukkan karakteristik serangan UDPLag yang didominasi paket kecil namun intensif.

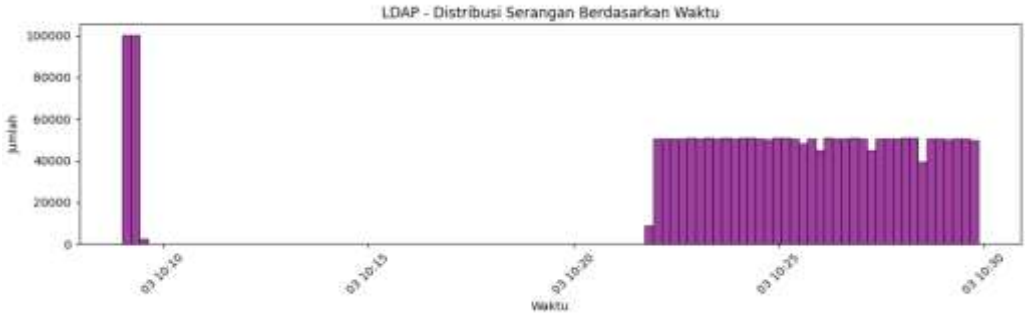


Gambar 5. Histogram dan boxplot ukuran paket Portmap

Gambar 5 memperlihatkan distribusi ukuran paket serangan Portmap menggunakan histogram (kiri) dan boxplot (kanan). Histogram menunjukkan mayoritas paket terkonsentrasi pada ukuran kecil, sedangkan boxplot menampilkan adanya beberapa outlier dengan ukuran paket yang jauh lebih besar, bahkan mendekati 20.000 Total Fwd Packets. Pola ini menggambarkan serangan Portmap yang umumnya menggunakan paket kecil namun disertai sejumlah paket berukuran sangat besar.

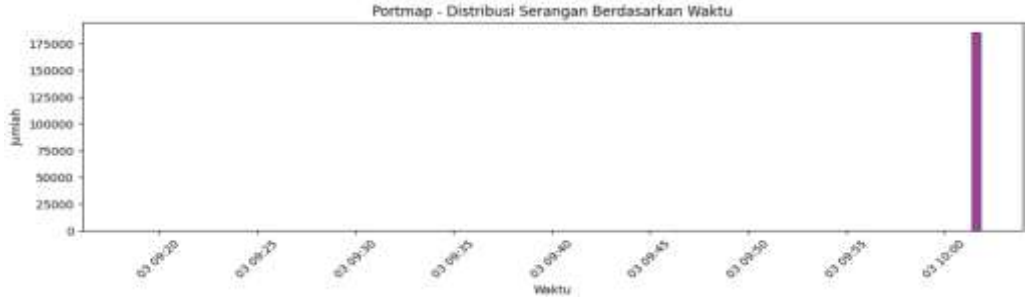
Visualisasi Intensitas Waktu Serangan

Distribusi serangan berdasarkan waktu menunjukkan bahwa LDAP memiliki serangan yang tersebar lebih luas, sedangkan UDPLag dan Portmap memiliki karakteristik berupa **lonjakan sesaat (spike)** yang mengindikasikan teknik flooding.



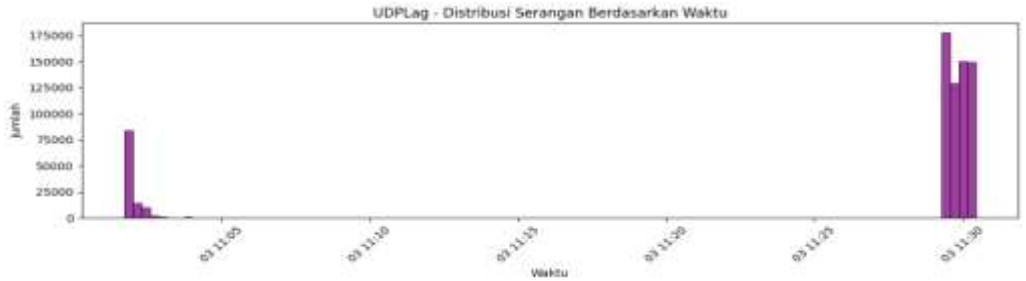
Gambar 6. Distribusi waktu serangan LDAP

Gambar 6 memperlihatkan distribusi waktu serangan LDAP. Terlihat bahwa aktivitas serangan terjadi secara bertahap, dimulai dengan lonjakan tajam pada awal waktu, kemudian berlanjut dengan sebaran serangan yang relatif merata pada rentang waktu berikutnya. Pola ini mengindikasikan bahwa serangan LDAP cenderung berlangsung persisten dalam periode yang cukup lama.



Gambar 7. Distribusi waktu serangan Portmap

Gambar 7 memperlihatkan distribusi waktu serangan Portmap. Aktivitas serangan terlihat terkonsentrasi pada satu titik waktu tertentu dengan lonjakan tajam, yang menunjukkan bahwa serangan Portmap dilakukan dalam waktu singkat (*spike*) dan tidak merata sepanjang periode pengamatan.



Gambar 8. Distribusi waktu serangan UDPLag

Gambar 8 menunjukkan distribusi waktu serangan UDPLag yang ditandai dengan beberapa lonjakan aktivitas (spike) pada interval waktu tertentu. Pola ini mengindikasikan bahwa serangan UDPLag dilakukan secara berulang dengan intensitas tinggi pada periode pendek, bukan secara merata sepanjang waktu.

Pemetaan CVE dan Evaluasi Risiko

Untuk mengevaluasi tingkat risiko dari setiap jenis serangan DDoS yang dianalisis, dilakukan pemetaan terhadap Common Vulnerabilities and Exposures (CVE). Hasil analisis menunjukkan bahwa serangan UDPLag terkait dengan CVE-2020-25705, yaitu kerentanan pada

kernel Linux yang memungkinkan paket ICMP Redirect dimanipulasi untuk mengeksploitasi sistem, dengan tingkat keparahan tinggi namun dampak serangan dinilai sedang (NVD, 2020).

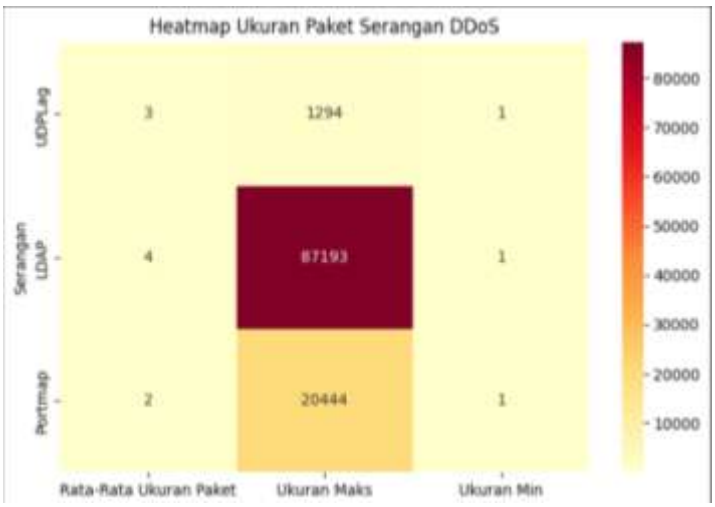
Sementara itu, serangan LDAP diasosiasikan dengan CVE-2016-2108, sebuah kerentanan pada protokol ASN.1 dalam OpenSSL yang memungkinkan serangan replay, namun memiliki tingkat urgensi rendah karena konteks eksploitasi yang terbatas (NVD, 2016).

Dalam hal Portmap, tingkat bahaya yang paling tinggi terkait dengan kerentanan yang dikenal sebagai CVE-1999-0500. Kerentanan ini melibatkan aktifitas layanan RPC (portmapper) secara tidak aman pada port 111, yang memungkinkan penyerang untuk mengenumerasi layanan RPC dan mengekspos sistem terhadap berbagai serangan khusus, yang membuatnya diklasifikasikan sebagai tingkat urgensi tinggi (NVD, 1999).

Melalui pemetaan ini, dapat ditarik kesimpulan bahwa meskipun LDAP menghasilkan volume data serangan terbesar, serangan Portmap justru menunjukkan tingkat ancaman tertinggi secara teknis berdasarkan CVE yang relevan.

Perbandingan Statistik Lanjutan

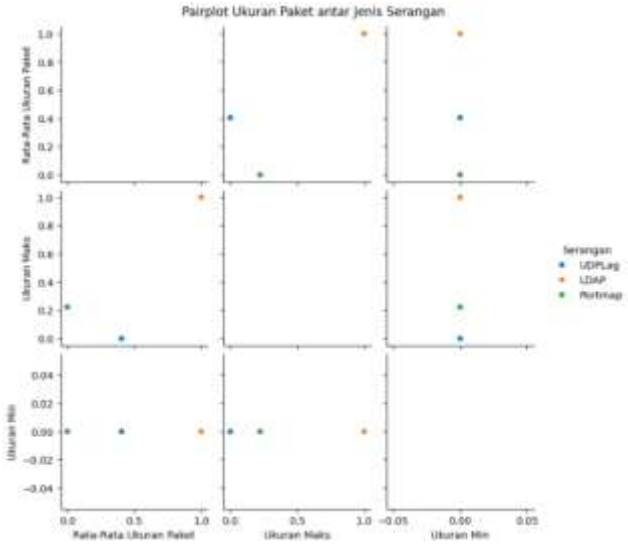
Heatmap digunakan untuk menggambarkan perbedaan nilai statistik antar serangan secara visual:



Gambar 9. Heatmap nilai rata-rata, maksimum, dan minimum ukuran paket untuk ketiga jenis serangan

Gambar 9 menampilkan heatmap yang membandingkan nilai rata-rata, maksimum, dan minimum ukuran paket dari ketiga jenis serangan DDoS. Terlihat bahwa serangan LDAP memiliki ukuran maksimum tertinggi (87.193), diikuti oleh Portmap (20.444) dan UDPLag (1.294). Meskipun ketiganya memiliki ukuran minimum yang sama, variasi nilai maksimum dan rata-rata menunjukkan perbedaan karakteristik dalam intensitas dan skala serangan.

Selain itu, *pairplot* memperlihatkan bahwa serangan LDAP menyimpang paling jauh dari distribusi lainnya, menjadikannya sebagai *outlier* dalam konteks ukuran paket dan intensitas.

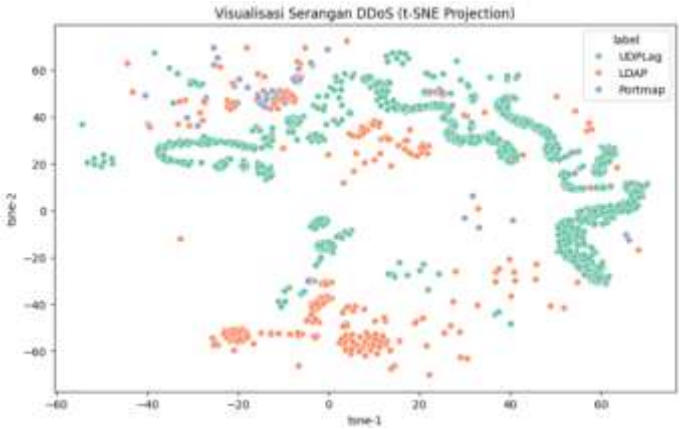


Gambar 10. Pairplot antar metrik ukuran paket (mean, max, min)

Gambar 10 memperlihatkan pairplot hubungan antar metrik ukuran paket (mean, max, min) untuk ketiga jenis serangan. Titik data menunjukkan bahwa serangan LDAP cenderung menyebar jauh dari dua jenis serangan lainnya, menandakan adanya perbedaan signifikan pada distribusi ukuran paket. Sementara itu, UDPLag dan Portmap terlihat lebih berdekatan, menunjukkan kemiripan dalam pola ukuran paket meskipun terdapat perbedaan pada nilai maksimumnya.

Visualisasi Reduksi Dimensi

Untuk Untuk mempermudah identifikasi pola antar jenis serangan, digunakan teknik *t-distributed Stochastic Neighbor Embedding* (t-SNE), sebuah metode reduksi dimensi yang efektif dalam memetakan data berdimensi tinggi ke dalam dua dimensi secara visual, terutama ketika terdapat hubungan non-linear antar fitur. Visualisasi hasil proyeksi menunjukkan bahwa serangan UDPLag dan Portmap cenderung membentuk kelompok (cluster) yang saling berdekatan, menandakan adanya kemiripan karakteristik antar keduanya. Sebaliknya, serangan LDAP tampak tersebar lebih luas di berbagai area ruang visual, yang mengindikasikan tingkat keragaman pola serangan yang lebih tinggi dan kemungkinan kompleksitas internal yang lebih besar. Meskipun visualisasi ini bersifat eksploratif dan belum divalidasi secara kuantitatif menggunakan metrik seperti silhouette score atau Davies-Bouldin Index, hasil ini memberikan wawasan awal yang berguna dalam memahami perbedaan distribusi dan struktur serangan secara menyeluruh.



Gambar 11. Visualisasi t-SNE ketiga jenis serangan DdoS

Gambar 11 Visualisasi t-SNE digunakan untuk memproyeksikan fitur berdimensi tinggi dari dataset serangan DDoS ke dalam dua dimensi (t-SNE 1 dan t-SNE 2), sehingga pola dan keterpisahan antar jenis serangan lebih mudah diamati. Dalam visualisasi ini, tiga jenis serangan DDoS—UDPLag, LDAP, dan Portmap—ditandai dengan warna berbeda. Terlihat bahwa ketiga jenis serangan membentuk klaster yang relatif terpisah, menunjukkan bahwa karakteristik fitur dari masing-masing serangan memiliki perbedaan yang signifikan. Ini mendukung efektivitas metode t-SNE dalam eksplorasi data dan validasi awal terhadap kemampuan model klasifikasi dalam membedakan jenis serangan.

Pembahasan

Penelitian ini bertujuan untuk melakukan analisis komparatif terhadap tiga jenis serangan Distributed Denial of Service (DDoS), yaitu UDPLag, LDAP, dan Portmap, dengan menggunakan dataset CIC-DDoS2019. Fokus utama pembahasan terletak pada karakteristik teknis dari masing-masing jenis serangan, mencakup distribusi ukuran paket, intensitas waktu serangan, serta evaluasi tingkat risiko berdasarkan klasifikasi Common Vulnerabilities and Exposures (CVE). Dari sisi ukuran paket, hasil analisis statistik deskriptif menunjukkan bahwa serangan LDAP memiliki nilai maksimum ukuran paket tertinggi, yakni sebesar 87.193 bytes. Nilai ini jauh melebihi Portmap (20.444 bytes) dan UDPLag (1.294 bytes). Rata-rata dan median ukuran paket LDAP juga lebih besar, menandakan bahwa serangan ini cenderung menggunakan lebih banyak bandwidth. Visualisasi melalui histogram dan boxplot menunjukkan bahwa LDAP mengandung sejumlah outlier ekstrem, sedangkan dua jenis serangan lainnya relatif terkonsentrasi pada ukuran paket kecil hingga sedang.

Berdasarkan distribusi waktu serangan, LDAP menunjukkan pola penyebaran yang lebih merata selama periode perekaman data berdasarkan distribusi waktu serangan, yang menunjukkan bahwa serangan ini dapat berlangsung lama. Sebaliknya, serangan UDPLag dan Portmap menunjukkan ciri lonjakan sesaat (spike), yang biasanya ditemukan dalam teknik lonjakan. Hasil ini menunjukkan bahwa strategi untuk masing-masing serangan berbeda: LDAP lebih tersebar dan persisten, sedangkan UDPLag dan Portmap lebih kuat dan cepat. Setiap serangan dipetakan ke dalam entri CVE yang relevan untuk mengevaluasi ancaman keamanan. Serangan UDPLag dikaitkan dengan kerentanan pada kernel Linux bernama CVE-2020-25705, yang memungkinkan pengendalian ICMP Redirect meskipun tingkat keparahannya tinggi, dalam konteks ini dikategorikan sebagai risiko sedang. Serangan LDAP dikaitkan dengan CVE-2016-2108, yaitu kerentanan pada protokol ASN.1 dalam OpenSSL dengan tingkat urgensi rendah karena kondisi eksploitasi yang lebih terbatas. Sementara itu, Portmap terhubung dengan CVE-1999-0500, sebuah kerentanan klasik pada port RPC 111 yang memungkinkan enumerasi layanan oleh penyerang, dan dikategorikan memiliki tingkat risiko tertinggi. Berdasarkan pemetaan ini, meskipun serangan LDAP memiliki volume data terbesar, Portmap menjadi jenis serangan dengan ancaman teknis paling kritis. Analisis statistik lanjutan menggunakan heatmap memperkuat temuan sebelumnya. LDAP secara konsisten mencatatkan nilai tertinggi dalam ukuran rata-rata, maksimum, dan minimum. Pairplot memperlihatkan bahwa LDAP menyimpang jauh dari distribusi dua jenis serangan lainnya, menjadikannya outlier dalam konteks metrik ukuran paket dan intensitas.

Terakhir, visualisasi dengan t-SNE digunakan untuk menyederhanakan dimensi data agar pola distribusi antar serangan dapat diamati lebih jelas. Hasil visualisasi menunjukkan bahwa UDPLag dan Portmap membentuk kelompok (cluster) yang saling berdekatan, sementara LDAP memiliki pola penyebaran yang lebih luas. Hal ini menunjukkan bahwa serangan LDAP memiliki keragaman karakteristik internal yang lebih tinggi dan dapat lebih sulit untuk diprediksi dibanding dua jenis serangan lainnya.

KESIMPULAN

Penelitian ini melakukan analisis komparatif terhadap tiga jenis serangan DDoS seperti UDPLag, LDAP, dan Portmap menggunakan dataset CIC-DDoS2019. Hasil studi menunjukkan bahwa masing-masing jenis serangan memiliki karakteristik teknis dan tingkat risiko yang berbeda, yang berimplikasi langsung terhadap strategi mitigasi yang perlu diterapkan. Serangan LDAP menonjol dari sisi ukuran dan volume paket tertinggi, serta menunjukkan penyebaran serangan yang lebih merata dalam waktu, mengindikasikan sifat serangan yang persisten dan intensif dalam penggunaan bandwidth. Sebaliknya, UDPLag dan Portmap menunjukkan lonjakan trafik dalam waktu singkat (spike) yang khas pada teknik flooding.

Dari sisi keamanan, pemetaan terhadap *Common Vulnerabilities and Exposures* (CVE) menempatkan Portmap sebagai serangan dengan tingkat risiko tertinggi, karena terkait dengan CVE-1999-0500 yang memungkinkan eksploitasi layanan RPC. Meski LDAP menghasilkan volume terbesar, tingkat kerentanannya lebih rendah berdasarkan eksploitasi yang terbatas (CVE-2016-2108). UDPLag, yang terkait dengan CVE-2020-25705, menunjukkan risiko sedang. Visualisasi data melalui histogram, boxplot, heatmap, dan t-SNE memperkuat kesimpulan bahwa LDAP merupakan serangan dengan variabilitas dan intensitas tertinggi, namun Portmap lebih kritis secara teknis. Klasterisasi menunjukkan bahwa LDAP memiliki distribusi paling menyebar, mengindikasikan keragaman pola yang kompleks.

Dengan demikian, penelitian ini menyimpulkan bahwa strategi mitigasi DDoS harus disesuaikan dengan karakteristik spesifik dari tiap jenis serangan. Pendekatan visual analitik yang dikombinasikan dengan penilaian risiko berbasis CVE terbukti efektif dalam membantu pengambilan keputusan mitigasi yang lebih terarah dan kontekstual di lingkungan keamanan siber.

SARAN

Berdasarkan hasil temuan dan analisis dalam penelitian ini, terdapat beberapa saran yang dapat dijadikan rekomendasi guna meningkatkan ketahanan sistem digital pemerintah terhadap serangan Distributed Denial of Service (DDoS). Pertama, instansi pemerintah disarankan untuk mengimplementasikan sistem pemantauan lalu lintas jaringan secara real-time yang dilengkapi dengan fitur deteksi dini terhadap anomali atau lonjakan trafik mencurigakan. Upaya ini penting agar respons terhadap serangan dapat dilakukan dengan lebih cepat dan efisien. Kedua, strategi mitigasi perlu disusun secara prioritas berdasarkan tingkat urgensi dan risiko yang ditimbulkan oleh masing-masing jenis serangan, sebagaimana yang ditunjukkan melalui pemetaan terhadap Common Vulnerabilities and Exposures (CVE), bukan semata-mata berdasarkan volume lalu lintas yang dihasilkan.

Selanjutnya, peningkatan kapasitas bandwidth dan penerapan arsitektur jaringan berbasis load balancing juga perlu dipertimbangkan, terutama dalam mengantisipasi serangan jenis LDAP yang menghasilkan lalu lintas dalam jumlah besar. Selain itu, kolaborasi dengan penyedia layanan keamanan siber seperti Cloudflare, Telkom-CSIRT, atau penyedia anti-DDoS lainnya perlu diperkuat guna memperoleh proteksi berlapis dan akses terhadap teknologi mitigasi terbaru. Pemerintah juga perlu menyusun protokol standar operasional (SOP) dalam penanganan insiden siber secara komprehensif, serta melakukan simulasi serangan secara berkala untuk menguji kesiapan respons instansi terhadap serangan yang sesungguhnya.

Terakhir, penguatan kapasitas sumber daya manusia (SDM) dalam bidang keamanan siber merupakan aspek yang sangat krusial. Diperlukan pelatihan teknis secara rutin agar tim keamanan informasi dapat memahami karakteristik berbagai jenis serangan dan menanganinya secara tepat. Investasi pada peningkatan kompetensi SDM akan menjadi fondasi penting dalam memperkuat pertahanan siber nasional secara berkelanjutan.

DAFTAR PUSTAKA

Cloudflare. (2023). *Understanding DDoS attacks.* Retrieved from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Haq, M. F., & Santoso, H. B. (2023). Intrusion detection system for DDoS attack using CIC-DDoS2019 dataset with machine learning. *IFTECH: Information Technology Journal*, 7(1), 15–24. https://doi.org/10.33021/iftech.v7i1.2109

Khan, M. A., Nam, Y., & Kim, M. (2021). A flow-based hybrid feature selection approach for DDoS attack detection using machine learning. *Electronics,* 10(6), 721. https://doi.org/10.3390/electronics10060721

MITRE. (2024). Common Vulnerabilities and Exposures (CVE). Retrieved from https://cve.mitre.org

National Institute of Standards and Technology. (2020). CVE-2020-25705. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2020-25705

Netscout. (2023). Threat Intelligence Report: DDoS Attack Trends. Retrieved from https://www.netscout.com/threatreport

Niyaz, Q., Sun, W., & Javaid, A. Y. (2019). A deep learning based DDoS detection system in software-defined networking (SDN). *Electronics,* 8(8), 897. https://doi.org/10.3390/electronics8080897

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2019). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 108–116). https://doi.org/10.5220/0006639801080116

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Evaluating deep learning approaches to characterize and classify network traffic for DDoS detection. *Computers & Security,* 89, 101682. https://doi.org/10.1016/j.cose.2019.101682

Zhou, L., & Pezaros, D. P. (2019). Evaluation of machine learning classifiers for zero-day intrusion detection–A survey and guide. *ACM Computing Surveys (CSUR)*, 52(4), 1–36. https://doi.org/10.1145/3336141

Canadian Institute for Cybersecurity. (2019). CIC-DDoS2019 dataset. University of New Brunswick. https://www.unb.ca/cic/datasets/ddos-2019.html