Pengenalan Pola Serangan UDP Flood Menggunakan Metode *Signature Based Analysis*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

Bayu Ramadany

09011181823004

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

Pengenalan Pola Serangan UDP Flood Menggunakan Metode *Signature Based Analysis*

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh

Bayu Ramadany

09011181823004

Indralaya, 27 Juli 2022

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, MT., Ph.D., IPU.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 20 Juli 2022

Tim Penguji :

1. **Ketua Sidang** : **Ahmad Zarkasi, M.T.**
2. **Sekretaris Sidang** : **Adi Hermansyah, M.T.**
3. **Penguji Sidang** : **Ahmad Heryanto, M.T.**
4. **Pembimbing** : **Deris Stiawan, M.T., Ph.D., IPU**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawahi ini:

Nama	: Bayu Ramadany
NIM	: 09011181823004
Program Studi	: Sistem Komputer
Judul Penelitian	: Pengenalan Pola Serangan UDP Flood Menggunakan Metode *Signature Based Analysis*

Hasil Pengecekan *Software iThenticate/Turnitin*: 7%

Menyatakan bahwa laporan skripsi saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, 1Agustus 2022

Bayu Ramadany

09011181823004

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT, dengan karunia dan rahmat-Nya, penulis dapat menyelesaikan penulisan Proposal Tugas Akhir yang berjudul **"Pengenalan Pola Serangan UDP Flood Menggunakan Metode Signature Based Analysis".**

Pada laporan ini, penulis menjelaskan mengenai pola serangan untuk udp flood terhadap suatu topologi dengan disertai data-data yang diperoleh penulis saat melakukan penelitian data. Penulis berharap agar laporan ini dapat membantu dan bermanfaat bagi orang banyak.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan baik dan lancar.

2. Orang tua tercinta yang telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih untuk segala do'a, motivasi dan dukungannya baik moril, materil maupun spritual selama ini.

3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya

5. Bapak Deris Stiawan, MT., Ph.D., IPU. selaku Dosen Pembimbing Tugas Akhir 1 yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

6. Bapak Dr. Ir. Bambang Tutuko, M.T., selaku Pembimbing Akademik Jurusan Sistem Komputer.

8. Mbak Reni selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

9. Teman-teman Kaktus e-Sprot yaitu Deny, Jonathan, Wahyu, Shiro, dan Dhoni yang telah mengcarry saya

10. dan semua pihak yang telah membantu

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap penelitian tugas akhir ini bermanfaat dan berguna bagi khalayak.

Wassalamu'alaikum Wr. Wb.

Indralaya, Mei 2022
Penulis,

Bayu Ramadany
NIM. 09011181823004

PENGENALAN POLA SERANGAN UDP FLOOD MENGGUNAKAN METODE SIGNATURE BASED ANALYSIS

Bayu Ramadany (09011181823004)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwjaya
Email : Bayuramadany3@gmail.com

ABSTRAK

User Datagram Protocol (UDP) merupakan salah satu protokol pada Transport Layer TCP/IP yang mendukung komunikasi yang tidak andal (*unreliable*), tanpa koneksi (*Connectionless*). Penelitian ini berfokus pada pengenalan pola serangan UDP Flood dengan menganalisis atibut serangan pada data *anomaly*, dataset yang digunakan pada penelitian terdapat tiga skenario dimulai dari data normal, data serangan, dan data gabungan. Ekatrasi data dilakukan untuk menentukan atribut unik yang akan digunakan untuk mendeksi dengan menggunakan Snort IDS. Hasil yang didapatkan berupa pola serangan pada atribut *Total Length, Data Length, IP Destination, TTL, Content* dan penggunaan metode *signature based analysis* jauh lebih baik dibandingkan dengan rule default pada snort, dibuktikan dengan akurasi pada data serangan mencapai 99,983% dan akurasi sedangkan akurasi rule default snort hanya 94,524%

Kata Kunci : *DDoS, DoS, Rule Based Signature, UDP Flood, Snort*

UDP FLOOD ATTACK PATTERN RECOGNITION WITH SIGNATURE BASED ANALYSIS

Bayu Ramadany (09011181823004)
Department of Computer Engineering , Faculty of Computer Science, Sriwijaya University
Email: Bayuramadany3@gmail.com

ABSTRACT

User Datagram Protocol (UDP) is one of the protocols at the TCP/IP Transport Layer that supports unreliable, Connectionless communication. This study focuses on the pattern recognition of UDP Flood attacks by analyzing atibut attacks on anomaly data, the dataset used in the study there are three scenarios starting from normal data, Attack data, and combined data. Data extraction is done to determine the unique attributes that will be used to detect by using Snort IDS. The results obtained in the form of attack patterns on the attributes of Total Length, Data Length, IP Destination, TTL, Content and the use of signature based analysis method is much better than the default rule on snort, evidenced by the accuracy of the attack data reached 99.983% and accuracy while the accuracy of the default rule snort only 94.524%

Keywords : *DDoS, DoS, Rule Based Signature, UDP Flood, Snort*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan menjadi faktor yang sangatlah penting mulai dari sisi industri, email, media sosial maupun layanan elektronik dari universitas. Akhir-akhir ini banyak layanan website dan layanan jaringan menjadi target bagi peretas, peretas menggunakan berbagai metode serangan, salah satunya Distributed Denial of Service (DDoS) untuk memanfaatkan kerentanan yang dimiliki oleh suatu sistem tersebut. Salah satu Kerentan yang dimaksud yaitu peretas membanjiri resource sehingga pengguna lain menjadi sulit untuk mengakses suatu layanan web service misalnya, dan juga membuat sumber daya jaringan korban menjadi lambat[1].

Penelitian yang dilakukan oleh [2] mengungkapkan bahwa Network Layer adalah area yang paling rentan terhadap serangan Distributed Denial of Service (DDoS) yang menargetkan jaringan kabel dan nirkabel, dimana data besar di pompa untuk melakukan serangan. Sebagai contoh dari serangan pada network layer: ICMP flood, SYN flood.

Para peneliti [3][4] menjelaskan bahwa salah satu dari serangan Distributed Denial of Service (DDoS) yang terjadi yaitu UDP flood. User datagram protokol atau UDP adalah protokol jaringan tanpa sesi dan karena itu rentan terhadap serangan yang berbahaya. Dalam serangan UDP flood penyerang mengirimkan paket dalam jumlah yang besar ke port yang di targetkan sehingga dapat menghabiskan badwidth target tersebut.

Pada penelitian [5] tentang pengenalan pola serangan TCP FIN flood pada IOT dengan metode rule based signature analysis. Dataset yang digunakan yaitu ada tiga skenario yaitu: normal, attack dan normal-attack. pengujian pertama dilakukan dengan menggunakan Snort dan pengujian kedua dilakukan dengan menerapkan metode *rules based signature,* Hasilnya pola serangan dapat dikenali

dengan beberapa parameter seperti ip ttl, header length, ip length, tcp flags,window, tcp header, data length.

Pada penelitian [6] mengenai pengenalan pola serangan Ping flood menggunakan algoritma K-Means pada jaringan IoT. Dapat menyimpulkan bahwa serangan ping flood memanfaatkan kebebasan ICMP, yang memungkinkan pengguna untuk mengirim echo paket ke host. Hasilnya serangan tersebut dapat dikenali melalui atribut unik dari paket header, yaitu: panjang pada frame header dan flag pada IP header. Selama percobaan, dua alert terdeteksi yaitu: priority 2 dan priority 3.

Rule Based Signature dirancang untuk mendeteksi serangan yang dikenali dengan menggunakan pola atau karakteristik dari lalu lintas jaringan tertentu dalam serangan tersebut. Salah satu kelebihan dari teknik deteksi ini yaitu kemampuanya untuk mendeteksi semua serangan yang di kenali secara efektif tanpa menghasilkan banyak alarm palsu. Metode kedua yaitu deteksi anomaly based kemampuan metode yang satu ini dapat mendeteksi serangan yang tidak diketahui, namun masalah penting dengan teknik ini adalah memungkinkan tingkat alarm palsu (FAR) yang tinggi karena perilaku dari lalu lintas jaringan sebelumnya tidak di ketahui meskipun lalu lintas tersebut legal sehingga dapat dianggap serangan [7][8].

Pada penelitan [9] mengenai Penggunaan Metode Signatured Based Dalam Pengenalan Pola Serangan Di Jaringan Komputer, dengan metode yang di gunakan yaitu *signatured based* yang mampu mengenali pola serangan dan juga dalam mendeteksi serangan pada protokol TCP. Hasilnya mendapatkan akurasi sebesar 75% dan mampu mengenali pola serangan TCP flood dengan menemukan parameter atribut unik pada dataset.

Mengacu pada latar belakang yang telah di uraikan di atas, penelitian ini bertujuan membahas mengenai pengenalan pola serangan Denial of Service (DoS) yang diberi judul "**Pengenalan Pola Serangan UDP Flood Menggunakan Metode Signature Based Analysis**"

1.2 Tujuan

Tujuan dari penelitian ini yaitu :

1. Menganalisa pola serangan Denial of Service (DoS) dan Distributed Denial Of Service (DDoS) pada protokol User Datagram Protocol (UDP)
2. Mengaplikasikan *Intrusion Detection System* (IDS) sebagai program pendeteksi serangan UDP Flood
3. Mengimplementasikan *Rule Based Signature* sebagai metode dalam mengklasifikasikan pola serangan UDP Flood

1.3 Manfaat

Adapun manfaat yang bisa diambil dari penelitian ini:

1. Dapat membedakan data normal dan serangan pada protokol UDP
2. Dapat menganalisis pola dari paket serangan DoS maupun DDoS UDP Flood
3. Mampu mengenali atibut unik pada serangan UDP Flood
4. Sebagai referensi bagi para peneliti lain mengenai serangan Denial of Service

1.4 Perumusan Masalah

Mengacu pada penelitian [3][4] yang menyatakan bahwa salah satu serangan Distributed Denial of Service (DDoS) yang sering terjadi menargetkan pada protokol UDP, karena UDP adalah protocol yang tidak andal (*unreliable*), tanpa koneksi (*connectionless*) dan tidak menggunakan *three-way handshake.*

Oleh karena itu ada beberapa point perumusan masalah pada penelitian ini:

1. Bagaimana menganalisis atribut pola serangan UDP Flood pada dataset trafik lalu lintas jaringan
2. Bagaimana menerapkan metode Rule Based Signatured dalam mendeteksi serangan UDP Flood

1.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini **:**

1. Tidak membahas cara mencegah serangan tersebut
2. Tidak dilakukan pada jaringan enskripsi dan proteksi firewall

3. Tidak dilakukan pada lalu lintas jaringan real-time
4. Pengujian hanya dilakukan pada protokol UDP

1.6 Metodologi Penelitian

Pada penelitian ini menggunakan metodologi sebagai berikut :

1. Metode Studi Pustaka dan Literature

   Pada metode ini mencari dan mengumpulkan referensi yang berupa literature yang terdapat pada buku, jurnal ilmiah, dan internet yang berkaitan dengan pembahasan Tugas Akhir ini.

2. Metode Konsultasi

   Pada metode ini melakukan konsultasi kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik terutama pembimbing dalam memberikan solusi permasalahan yang ditemui pada penelitian tugas akhir ini.

3. Metode Perancangan Software

   Dalam tahap ini dilakukan perancangan serta pembuatan sistem untuk mengenali pola serangan UDP Flood Denial of Service (DoS)

4. Metode Pengujian

   Pada metode ini akan dilakukan pengujian sistem dengan Batasan masalah dengan parameter yang telah ditentukan

5. Metode Analisa dan Kesimpulan

   Hasil dari pengujian pada tugas akhir ini akan dianalisis baik kelebihannya maupun kekurangannya dan juga menganalisis bagaimana hasil dari perancangan dan faktor penyebabnya sehingga dapat dilakukan pengembangan pada penelitian selanjutnya

1.7 Sistematika Penelitian

Berikut merupakan sistematika yang digunakan dalam penulisan penelitian tugas akhir agar dapat mendeskripsikan bab-bab penelitian yang terstruktur. Berikut susunan penelitian yang di gunakan yaitu:

BAB I PENDAHULUAN

Pada bab ini berisikan latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penelitian dari

penelitian yang di angkat, mengenai pengenalan pola serangan DoS UDP flood

BAB II TINJAUAN PUSTAKA

Bab ini berisikan dasar teori dari berbagai sumber yang akan dijadikan referensi penelitian meliputi literatur review yang berkaitan dengan masalah mengenai serangan DoS flood dengan menggunakan rule based signature

BAB III METODOLOGI PENELITIAN

Bab ini berisikan penjelasan bertahap dan rinci mengenai langkah-langkah yang digunakan untuk membuat rangka kerja dalam menyelesaikan penelitian tugas akhir ini

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan hasil dari pengujian yang dilakukan dan data yang diuji berdasarkan parameter yang ditentukan sebelumnya dan akan di analisa menggunakan teknik yang sesuai

BAB V KESIMPULAN

Bab ini berisikan penjelasan kesimpulan dari hasil penelitian yang telah dilakukan

Daftar Pustaka

[1] M. Alkasassbeh, G. Al-Naymat, A. B.A, and M. Almseidin, “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, 2016, doi: 10.14569/ijacsa.2016.070159.

[2] A. Munshi, N. A. Alqarni, and N. Abdullah Almalki, “DDOS Attack on IOT Devices,” *ICCAIS 2020 - 3rd Int. Conf. Comput. Appl. Inf. Secur.*, pp. 5–9, 2020, doi: 10.1109/ICCAIS48893.2020.9096818.

[3] S. Kalime, N. Boddula, A. Professor, and C. Science, “A Study on Detection of Distributed Denial of Service Attacks Using Machine Learning Techniques,” *Int. J. Res. Available*, pp. 5611–5620, [Online]. Available: https://edupediapublications.org/journals/index.php/IJR/.

[4] L. Huraj, M. Simon, and T. Horak, “IoT Measuring of UDP-Based Distributed Reflective DoS Attack,” *SISY 2018 - IEEE 16th Int. Symp. Intell. Syst. Informatics, Proc.*, pp. 209–214, 2018, doi: 10.1109/SISY.2018.8524703.

[5] D. Stiawan *et al.*, “TCP FIN flood attack pattern recognition on Internet of Things with rule based signature analysis,” *Int. J. online Biomed. Eng.*, vol. 15, no. 7, pp. 124–139, 2019, doi: 10.3991/ijoe.v15i07.9848.

[6] D. Stiawan *et al.*, “Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network,” *IEEE Access*, vol. 9, pp. 116475–116484, 2021, doi: 10.1109/ACCESS.2021.3105517.

[7] J. Alsamiri and K. Alsubhi, “Internet of things cyber attacks detection using machine learning,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, pp. 627–634, 2019, doi: 10.14569/ijacsa.2019.0101280.

[8] Z. S. Malek, B. Trivedi, and A. Shah, “User behavior pattern-signature based intrusion detection,” *Proc. World Conf. Smart Trends Syst. Secur. Sustain. WS4 2020*, vol. 7, pp. 549–552, 2020, doi:

10.1109/WorldS450073.2020.9210368.

[9] H. Setiawan, M. Agus Munandar, L. W. Astuti, and P. Korespondensi, "Penggunaan Metode Signatured Based Dalam Pengenalan Pola Serangan Di Jaringan Komputer," vol. 8, no. 3, pp. 517–524, 2021, doi: 10.25126/jtiik.202184200.

[10] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017, doi: 10.1016/j.jnca.2017.02.009.

[11] G. Ramadhan, Y. Kurniawan, and Chang-Soo Kim, "Design of TCP SYN Flood DDoS attack detection using artificial immune systems," pp. 72–76, 2017, doi: 10.1109/icsengt.2016.7849626.

[12] S. Usman, I. Winarno, and A. Sudarsono, "Implementation of SDN-based IDS to protect Virtualization Server against HTTP DoS attacks," *IES 2020 - Int. Electron. Symp. Role Auton. Intell. Syst. Hum. Life Comf.*, pp. 195–198, 2020, doi: 10.1109/IES50839.2020.9231699.

[13] S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, "DDoS Intrusion Detection Through Machine Learning Ensemble," *Proc. - Companion 19th IEEE Int. Conf. Softw. Qual. Reliab. Secur. QRS-C 2019*, pp. 471–477, 2019, doi: 10.1109/QRS-C.2019.00090.

[14] B. Habib, F. Khurshid, A. H. Dar, and Z. Shah, "DDoS Mitigation in Eucalyptus Cloud Platform Using Snort and Packet Filtering-IP-Tables," *2019 4th Int. Conf. Inf. Syst. Comput. Networks, ISCON 2019*, pp. 546–550, 2019, doi: 10.1109/ISCON47742.2019.9036183.

[15] A. L. Beena and S. Humayoon Kabir, "Defence mechanism for DoS attack in digital library (Using Citation Network)," *2019 Int. Conf. Intell. Comput. Control Syst. ICCS 2019*, no. Iciccs, pp. 1065–1068, 2019, doi: 10.1109/ICCS45141.2019.9065625.

[16] M. T. Naing, T. T. Khaing, and A. H. Maw, "Evaluation of TCP and UDP Traffic over Software-Defined Networking," *2019 Int. Conf. Adv. Inf.*

Technol. ICAIT 2019, pp. 7–12, 2019, doi: 10.1109/AITC.2019.8921086.

[17] C. Roja and P. N. Jayanthi, “Syslog Daemon for Security Event Monitoring using UDP Protocol,” *Proc. 3rd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2019*, pp. 1349–1354, 2019, doi: 10.1109/ICECA.2019.8821956.

[18] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, and V. Grout, “Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning,” *IEEE Access*, vol. 9, pp. 122495–122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[19] M. Qayyum, W. Hamid, and M. A. Shah, “Performance analysis of snort using network function virtualization,” *ICAC 2018 - 2018 24th IEEE Int. Conf. Autom. Comput. Improv. Product. through Autom. Comput.*, no. September, pp. 1–6, 2018, doi: 10.23919/IConAC.2018.8749024.

[20] R. T. Gaddam and M. Nandhini, “An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment,” *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2017*, no. Icicct, pp. 10–15, 2017, doi: 10.1109/ICICCT.2017.7975177.