PENGENALAN POLA SERANGAN *SLOW HTTP DOS* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION*

TUGAS AKHIR

Oleh :

Diah Komariah
09011181621018

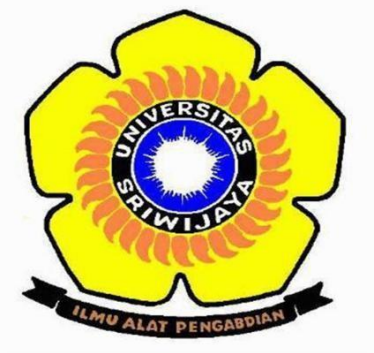
JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

PENGENALAN POLA SERANGAN *SLOW HTTP DOS* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer



Oleh :

Diah Komariah
09011181621018

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

PENGENALAN POLA SERANGAN *SLOW HTTP DOS* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

DIAH KOMARIAH
09011181621018

Indralaya, 22 Juni 2021

Pembimbing I Tugas Akhir

Deris Stiawan, M.T., Ph.D
NIP. 197806172006041002

Mengetahui,
Pembimbing II Tugas Akhir

Ahmad Heryanto, S.Kom., M.T
NIP. 198701222015041002

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:
Hari : Jumat
Tanggal : 30 April 2021

Tim Penguji:

1. **Ketua** : **Ahmad Zarkasi. S.T., M.T.** (.....)

2. **Penguji** : **Huda Ubaya, S.T., M.T.** (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, MT
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Diah Komariah

NIM : 09011181621018

Judul : Pengenalan Pola Serangan *Slow HTTP DoS* Dengan Menggunakan Metode *Regular Expression*

Hasil Pengecekan Software iThenticate/Turnitin : 2%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan / *plagiat*. Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku .

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak di paksakan.

Palembang, 22 Juni 2021

Diah Komariah

NIM.09011181621018

HALAMAN PERSEMBAHAN

"Sesungguhnya besama kesulitan pasti ada kemudahan. Maka apabila engkau telah selesai (dari suatu urusan), tetaplah berkerja keras (untuk urusan yang lain)"
(QS 94:6-7)

"Skripsi ini saya persembahkan sepenuhnya kepada dua orang hebat dalam hidup saya, Ayahanda dan Ibunda. Keduanya lah yang membuat segalanya menjadi mungkin sehingga saya bisa sampai pada tahap di mana skripsi ini akhirnya selesai. Terima kasih atas segala pengorbanan, nasihat dan doa baik yang tidak pernah berhenti kalian berikan kepadaku. Aku selamanya bersyukur dengan keberadaan kalian sebagai orangtua ku."

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat- Nya sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini dengan judul **"Pengenalan Pola Serangan *Slow HTTP DoS* dengan menggunakan Metode *Regular Expression*".**

Penulisan Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan tugas akhir ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Proposal Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Huda Ubaya, S.T., M.T. selaku Dosen Penguji pada Sidang Seminar Proposa (Tugas Akhir I) dan Sidang Kompre (Tugas Akhir II).
8. Orang Tua Ayah/Ibu yang selalu memberikan dukungan dan semangat saat mengerjakan tugas akhir.
9. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Almamater.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Proposal Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Palembang, 22 Juni 2021

Penulis

Diah Komariah

NIM. 09011181621018

PENGENALAN POLA SERANGAN *SLOW HTTP DOS* DENGAN MENGGUNAKAN METODE *REGULAR EXPRESSION*

Diah Komariah (09011181621018)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : diahkomariah505@gmail.com

ABSTRAK

Serangan *slow http dos* adalah salah satu metode serangan *DoS* yang menargetkan *server HTTP*. Metode ini menghambat layanan dengan membanjiri sehingga menimbulkan kumpulan koneksi dengan permintaan yang lambat dan banyak menuju *web server*. Diketahui bahwa serangan *slow HTTP DoS* oleh satu penyerang dapat dicegah secara efektif dengan membatasi jumlah koneksi untuk setiap alamat *IP*. Tujuan dari penelitian ini adalah untuk mendapatkan tingkat akurasi terbaik pada serangan *slow http dos* dengan menggunakan metode *regular expression* menggunakan dataset *IoT_Dataset_HTTP_DoS*. *Regular Expression* digunakan untuk mengenali atau mendeteksi suatu pola serangan tertentu pada suatu string. Pola serangan *slow http dos* pada dataset *DoS_HTTP* dapat dikenali dengan beberapa fitur seperti *Protocol, Port Destination, TTL, Source Port* dan juga *Payload*. Pada penelitian ini menunjukkan hasil yang sangat baik dengan nilai akurasi sebesar 99% yang menandakan keakuratan dalam pengenalan pola pada serangan *slow http dos* pada penelitian ini.

Kata kunci: *Slow HTTP DoS Attcks, Regular Expression, Snort IDS, Web Server, DoS (Denial of Service).*

Mengetahui

Pembimbing I	**Pembimbing II**
Deris Stiawan,M.T.,Ph.D	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP.198701222015041002**

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

Slow HTTP DoS Attack Pattern Recognition Using the Regular Expression Method

Diah Komariah (09011181621018)

Department of Computer Systems, Faculty of Computer Science,

Sriwijaya University

Email : diahkomariah505@gmail.com

ABSTRACT

Slow http dos attack is one of the DoS attack methods targeting HTTP servers. This method hampers the service by flooding it causing a pool of connections with slow and heavy requests to the web server. It is known that a slow HTTP DoS attack by a single attacker can be effectively prevented by limiting the number of connections for each IP address. The purpose of this study is to obtain the best level of accuracy in slow http dos attacks by using the regular expression method using the IoT_Dataset_HTTP_DoS dataset. Regular Expression is used to recognize or detect a certain attack pattern on a string. The slow http dos attack pattern on the DoS_HTTP dataset can be recognized by several features such as Protocol, Destination Port, TTL, Source Port and Payload. This study shows very good results with an accuracy value of 99% which indicates the accuracy in pattern recognition in slow http dos attacks in this study.

Keywords: *Slow HTTP DoS Attcks, Regular Expression, Snort IDS, Web Server, DoS (Denial of Service).*

Mengetahui

Pembimbing I	**Pembimbing II**
Deris Stiawan,M.T.,Ph.D	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP.198701222015041002**

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Serangan *slow http dos* adalah salah satu metode serangan *dos* terhadap *server HTTP* dan menjadi salah satu ancaman yang mengirimkan sejumlah permintaan palsu atau tidak nyata kedalam *host* atau *server* jaringan.

Serangan *Denial of Service* umumnya dilakukan membanjiri server atau host sehingga *host* korban kehabisan sumber daya (memori, CPU, lalu lintas). Kondisi ini membuatnya tidak dapat melayani pengguna lain. *Flooding* atau membanjiri sulit diatasi, tidak cukup hanya dengan *me-reboot*, seperti serangan lainnya. Serangan *slow http dos* ini adalah salah satu metode serangan *DoS* terhadap *server HTTP*.

Regular Expression adalah *string* yang berisi kombinasi karakter normal dan metakarakter khusus atau *metasequences*. Metakarakter dan *metasequences* adalah karakter atau urutan karakter yang merepresentasikan ide seperti kuantitas, lokasi, atau jenis karakter[1]. Bagian selanjutnya mencantumkan ketersediaan dan sintaks untuk karakter meta yang didukung untuk implementasi *regular expression* tertentu.

Pencocokan pola memungkinkan penjabaran teks ukuran besar dengan cepat untuk dapat menemukan pola tertentu untuk mengedit maupun mengekstrak juga menghapus *substring* teks[2]. Pada aplikasi yang banyak memproses string seperti pemrosesan html , penguraian file , juga penguraian httpyang lebih sulit.

Server web adalah *software* yang akan berjalan di sisi *server* bertugas untuk menerima permintaan dari *web*, kemudian menerjemahkan permintaan tersebut, dan hasil dari permintaan itu akan dikembalikan ke web[3]. Menurut[4] *server web* merupakan teknologi untuk mengubah kemampuan internet dengan menambahkan kemampuan *web transaksional*, yaitu kemampuan *web* untuk saling berkomunikasi dengan pola *program-to-program (P2P)*.

Salah satu serangan yang dapat di lakukan di *web server*[5] yaitu *Slow HTTP DoS (Denial of Service)* Dengan menargetkan *server HTTP*, metode ini memblokir layanan dengan membanjirinya, mengakibatkan sejumlah besar koneksi *server web* yang lambat.

Perangkat lunak yang digunakan pada *web server* terletak pada komputer *server* sebagai lokasi penyimpanan data *website*. Cara kerja *web server* sangat sederhana, yaitu menerima permintaan klien dan kemudian mengirimkannya kembali ke klien dalam bentuk file. Ketika klien atau browser meminta data dari *server web,* permintaan data tersebut akan dikemas dan kemudian dikirim ke alamat yang diperlukan, seperti *HTTP* atau *HTTPS.*

Ketika penyerang mencoba menembus jaringan, ada banyak sistem pertahanan, termasuk sistem deteksi *intrusi (IDS)*. Sebagian besar *IDS* mampu mendeteksi banyak serangan, tetapi tidak dapat memberikan gambaran yang jelas kepada analis karena banyaknya peringatan palsu yang dihasilkan oleh sistem ini[6]. Kelemahan *IDS* ini telah menyebabkan munculnya banyak metode untuk menangani peringatan ini, meminimalkannya, dan menyoroti serangan yang sebenarnya.

Pada penelitian[7] yang telah melakukan *klasifikasi* dengan menggunakan dataset *KDD CUP 1999* hasil akurasi tertinggi pada pengujian ini sebesar 90% pada saat jumlah data *training* 3000 data *testing* 150 dengan menggunakan nilai K.

Pada tugas akhir kali ini akan melakukan penelitian tentang pengenalan pola serangan *slow http dos* pada suatu web sever menggunakan dataset "*Dataset_HTTP_DoS*" yang telah dibuat pada tahun 2018 menggunakan metode *regular expression* dan berharap dapat mendapatkan akurasi yang lebih besar dari metode-metode sebelumnya.

1.2 Tujuan

Tujuan dari penulisan tugas akhir ini yaitu :

1. Menerapkan metode *Regex* digunakan untuk mendeteksi serangan.
2. Memahami *pattern* dari serangan *slow http DoS* di *web server.*
3. Menjelaskan cara kerja dari serangan *slow http DoS* di *web server.*

1.3 Manfaat

Manfaat dari penulisan Tugas Akhir ini yaitu :

1 . Memberikan informasi mengenai sistem kerja dari serangan *slow http DoS.*

2 . Memberikan informasi mengenai cara menerapkan Metode *RegEx* (*Regular Expression)* .

3. Membagikan informasi tentang akurasi yang didapat dari metode *regular expression.*

1.4 Rumusan Masalah

Rumusan masalah pada tugas akhir ini yaitu :

1. Bagaimana serangan *slow http DoS* bisa terjadi pada *web server* dengan menggunakan metode *RegEx* ?
2. Bagaimana pola yang telah didapat dari serangan *slow http DoS ?*
3. Bagaimana cara mendapatkan *performa* terbaik dengan menerapkan metode *RegEx* ?

1.5 Batasan Masalah

Batasan masalah pada tugas akhir ini sebagai berikut :

1. Penelitian yang akan dilakukan *web server* berkarakter *private/public*.
2. Metode yang akan digunakan untuk menganalisis data memakai metode *RegEx.*
3. *Sistem Snort* digunakan untuk memeriksa apakah adanya serangan di *web server.*
4. Data yang akan dipakai diperoleh dari *tools slowloris.pl.*

1.6 Metodologi Penelitian

Metodologi penelitian ini sejumlah langkah yaitu :

Metodologi yang digunakan dalam penulisan tugas akhir ini akan melewati beberapa tahapan sebagai berikut :

1. Perumusan Masalah

Dalam tahap ini penulis melakukan pengujian dengan menggunakan *tools slowloris* untuk melakukan serangan dan membuktikan adanya serangan pada *web server.*

2. *Study Referensi*

Tahapan kedua , penulis akan mencari beberapa informasi yang akan digunakan untuk pembelajaran melewati media *website* yang terpercaya yaitu penelitian, juga tulisan yang berkaitan, serta melakukan konsultasi kepada orang-orang yang dianggap memiliki pengetahuan dan wawasan tentang penelitian tersebut untuk membantu penyusunan tugas akhir kali ini .

3. Penyusunan memakai metode *RegEx*

Pada tahapan ketiga, akan di lakukan penyusunan skema sesuai apa yang ada pada rumusan masalah penelitian ini. Pada tahapan ketiga membangun terlebih dahulu *web server* untuk melakukan penyerangan menggunakan tools *slowloris.pl* .

4. Pengujian

Pada tahap keempat ini akan dilakukannya pengujian dari *tools slowloris* yang sudah didapat . Di tahap ini serangan *slow http DoS* akan di ujikan menggunakan *ubuntu* pada *web server* .

5. Analisis

Pada tahapan kelima adalah akan menganalisis hasil dari penelitian. Di tahap kelima akan dianalisis seperti apa serangan itu akan dijelaskan secara detail.

6. Kesimpulan

Pada kesimpulan ini hasil dari penelitian pada metode yang di uji akan dianalisa dengan tujuan mengetahui kekurangan pada hasil penelitian dan sebagai. *Referensi* untuk pengembangan pada penelitian selanjutnya.

1.7 Sistematika Penulisan

Untuk memudahkan dalam menyusun tugas akhir ini juga memperjelas isi dari bab yang ada pada laporan ini , maka akan dibuat sistem penulisan yaitu :

BAB I PENDAHULUAN

Bab I ini berisi penjelasan dari *background,* tujuan, manfaat, rumusan masalah,batasan masalah, metodologi penelitian dan juga sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab II ini mengandung teori dari *Slow HTTP DoS, Network Forensic RegEx (Regular Expression) ,Web Server,Snort , DoS (Denial of Service)* yang berhubungan pada penulisan ini.

BAB III METODOLOGI

Pada Bab ini membicarakan mengenai proses dari penelitian yang akan dikerjakan. Penjabaran akan memaparkan beberapa tahap seperti rancangan sistem juga menerapakan struktur penelitian yang dipakai pada tugas akhir ini.

BAB IV PENGUJIAN DAN ANALISIS

Pada Bab IV ini hasil penelitian ini akan dianalisis dari serangan *Slow HTTP DoS* yang telah dilakuakan di *web server*.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisikan beberapa *referensi* dari setiap bab yang telah dibahas juga akan berisikan masukan untuk penelitian selanjutnya .

DAFTAR PUSTAKA

[1] X. Wang *et al.*, "Hyperscan : A Fast Multi-pattern Regex Matcher for Modern CPUs This paper is included in the Proceedings of the," 2019.

[2] M. Becchi, A. Bremler-Barr, D. Hay, O. Kochba, and Y. Koral, "Accelerating regular expression matching over compressed HTTP," *Proc. - IEEE INFOCOM*, vol. 26, no. July 2014, pp. 540–548, 2015, doi: 10.1109/INFOCOM.2015.7218421.

[3] R. Dawood, S. F. Qiana, and S. Muchallil, "Kelayakan Raspberry Pi sebagai Web Server: Perbandingan Kinerja Nginx, Apache, dan Lighttpd pada Platform Raspberry Pi," *J. Rekayasa Elektr.*, vol. 11, no. 1, pp. 25–29, 2014, doi: 10.17529/jre.v11i1.1992.

[4] Y. D. Setiyawati, R. R. Isnanto, and K. T. Martono, "Pembuatan Aplikasi Antar-Jemput Laundry Berbasis Web Service pada Platform Android," *J. Teknol. dan Sist. Komput.*, vol. 4, no. 1, p. 150, 2016, doi: 10.14710/jtsiskom.4.1.2016.150-158.

[5] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," vol. 7, no. 1, pp. 56–70, 2020.

[6] S. Upadhyay and R. R. Singh, "A Survey on IDS Alerts Classification Techniques," *Int. J. Comput. Appl.*, vol. 105, no. 12, pp. 975–8887, 2014.

[7] Y. Ariyanto, V. Al, H. Firdaus, and H. Pramana, "Klasifikasi Jenis serangan DOS dan Probing pada IDS menggunakan metode K- Nearest Neighbor," vol. 3, pp. 1–5, 2020.

[8] C. L. Calvert and T. M. Khoshgoftaar, "Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data," *J. Big Data*, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0230-3.

[9] Y. Xie and S. Z. Yu, "Monitoring the application-layer DDoS sttacks for popular websites," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 15–25, 2009, doi: 10.1109/TNET.2008.925628.

[10] G. Maciá-Fernández, J. E. Díaz-Verdejo, P. García-Teodoro, and F. De Toro-Negro, "LoRDAS: A low-rate DoS attack against application servers," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5141 LNCS, pp. 197–209, 2008, doi: 10.1007/978-3-540-89173-4_17.

[11] M. Almgren, H. Debar, and M. Dacier, "A Lightweight Tool for Detecting Web Server Attacks.," *Ndss*, no. March, pp. 1–14, 2000.

[12] S. E. Salama, M. I. Marie, L. M. El-Fangary, and Y. K. Helmy, "Web Server Logs Preprocessing for Web Intrusion Detection," *Comput. Inf. Sci.*, vol. 4, no. 4, pp. 123–133, 2011, doi: 10.5539/cis.v4n4p123.

[13] L. K. Joshila Grace, V. Maheswari, and D. Nagamalai, “Analysis of Web Logs And Web User In Web Mining,” *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 1, pp. 99–110, 2011, doi: 10.5121/ijnsa.2011.3107.

[14] E. Casey, “Network traffic as a source of evidence: Tool strengths, weaknesses, and future needs,” *Digit. Investig.*, vol. 1, no. 1, pp. 28–43, 2004, doi: 10.1016/j.diin.2003.12.002.

[15] E. Larson and A. Kirk, “Generating Evil Test Strings for Regular Expressions,” *Proc. - 2016 IEEE Int. Conf. Softw. Testing, Verif. Validation, ICST 2016*, pp. 309–319, 2016, doi: 10.1109/ICST.2016.29.

[16] C. Chapman and K. T. Stolee, “Exploring regular expression usage and context in python,” *ISSTA 2016 - Proc. 25th Int. Symp. Softw. Test. Anal.*, pp. 282–293, 2016, doi: 10.1145/2931037.2931073.

[17] C. A. Staicu and M. Pradel, “Freezing the web: A study of ReDoS vulnerabilities in JavaScript-based web servers,” *Proc. 27th USENIX Secur. Symp.*, pp. 361–376, 2018.

[18] S. Allesina and M. Wilmes, “5. Regular Expressions,” *Comput. Ski. Biol.*, vol. 11, no. 4, pp. 165–184, 2019, doi: 10.1515/9780691183961-009.

[19] Yogi, I. Ruslianto, and S. Bahri, “Analisa Log Web Server Untuk Mengetahui Pola Perilaku Pengunjung Website Menggunakan Teknik Regular Expressions,” *J. Komput. dan Apl.*, vol. 07, no. 01, pp. 120–130, 2019.

[20] E. Ophie, “Aplikasi Algoritma String Matching dan Regex untuk Validasi Formulir,” *Apl. Algoritm. String Matching dan Regex untuk Validasi Formulir*, 2014.

[21] J. E. Siswosubroto, A. A. E. Sinsuw, X. B. N. Najoan, and J. T. Elektro-ft, “Analisa dan Perancangan Arsitektur Jaringan Balai Teknik Kesehatan Lingkungan dan Penanggulangan Penyakit (BTKLPP),” vol. 4, no. 5, pp. 37–43, 2015.

[22] O. A. Osanaiye and M. Dlodlo, “TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment,” *Proc. - EUROCON 2015*, pp. 0–5, 2015, doi: 10.1109/EUROCON.2015.7313736.

[23] T. Berbasis, I. P. Di, P. T. Indosat, C. Malang, A. T. P. T. Indosat, and T. B. K. M. Branch, “Tradisional Untuk Jaringan Perangkat the Analysis of Diffserv Implementation in Traditional.”

[24] P. S. Informatika, “Perancangan Private Cloud Storage Menggunakan ownCloud (Studi Kasus di Program Studi Magister Ilmu Lingkungan Universitas Sebelas Maret)Perancangan Private Cloud Storage Menggunakan ownCloud (Studi Kasus di Program Studi Magister Ilmu Lingkungan Unive,” 2014.

[25] M. Affandi and S. Setyowibowo, “Implementasi Snort Sebagai Alat Pendeteksi Intrusi,” *Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux*, vol. 4, no. 2, 2013.

[26] M. Arman and N. Rachmat, “Implementasi Sistem Keamanan Web Server Menggunakan Pfsense,” *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 1, pp. 13–23, 2020, doi: 10.32767/jusikom.v5i1.752.

[27] 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.

[28] T. M. Aji, D. E. Riyanto, and H. A. Wibawa, “PENERAPAN WEB SERVICES DAN REGULAR EXPRESSION UNTUK VERIFIKASI ALAMAT BERBASIS HASIL PENELUSURAN,” vol. 1, no. 1, pp. 38–51, 2012.

[29] Z. Trabelsi and L. Alketbi, “Using network packet generators and snort rules for teaching denial of service attacks,” *Annu. Conf. Innov. Technol. Comput. Sci. Educ. ITiCSE*, pp. 285–290, 2013, doi: 10.1145/2462476.2465580.

[30] K. L. Sutherland and H. Date, “3. モンテカルロシミュレーションの放射線医療への応用 1 2 3,” *Pros. Semin. Nas. Apl. Sains Teknol.*, vol. 70, no. 8, pp. 827–838, 2014.

[31] M. F. Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 9, pp. 3112–3123, 2018.

[32] R. Davidrajuh and C. Rong, “Solving Scheduling Problems with Randomized and Parallelized Brute-Force Approach,” *12th Int. Conf. Comput. Sci. Inf. Technol. CSIT 2019*, pp. 1–4, 2019, doi: 10.1109/CSITechnol.2019.8895104.

[33] B. H. Izza, Khaerani. Lekso, “Implementasi Dan Analisa Hasil Data Mining Untuk Klasifikasi Serangan Pada Intrusion Detection (Ids) Dengan Algoritma C4.5,” *Techno.COM*, vol. 14, no. 3, pp. 181–188, 2015.