SISTEM PENCEGAHAN SERANGAN DDOS UDP FLOODING DENGAN METODE STRING MATCHING SECARA REAL-TIME

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

RAHMAN RAMADHAN
09011381621082

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

SISTEM PENCEGAHAN SERANGAN DDOS UDP FLOODING DENGAN METODE STRING MATCHING SECARA REAL-TIME

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

RAHMAN RAMADHAN
09011381621082

Palembang, Agustus 2020

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

Mengetahui,
Ketua Jurusan

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at
Tanggal : 7 Agustus 2020

Tim Penguji :

1. **Ketua** : **Ahmad Zarkasih, S.T., M.T.**
2. **Sekretaris I** : **Deris Stiawan, Ph. D.**
3. **Sekretaris II** : **Ahmad Heryanto, S.Kom., M.T.**
4. **Anggota I** : **Huda Ubaya, S.T., M.T.**
5. **Anggota II** : **Sarmayanta Sembiring, S.Si., M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Rahman Ramadhan
Nim : 09011381621082
Judul : Sistem Pencegahan Serangan DDoS UDP Flooding dengan Metode String Matching Secara Real-Time

Hasil Pengecekan *Software iThenticate / Turnitin* : 4%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsru 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 dipaksakan.

Palembang, Agustus 2020
Yang menyatakan,

Rahman Ramadhan

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"Sistem Pencegahan Serangan DDoS UDP Flooding dengan Metode String Matching Secara Real-Time"**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang inshaAllah istiqomah hingga akhir zaman.

Selesainya penyusunan Proposal Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusun Proposal Tugas Akhir ini.
2. Orangtua tercinta, yaitu Bapak Hendra Halik dan Ibu Lusiana, serta saudara penulis, yaitu Adi Yudha Pratama dan Amran Ismail, serta keluarga besar penulis yang tersayang.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, Ph. D. selaku Pembimbing I Tugas Akhir.
5. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing II Tugas Akhir.
6. Ibu Sri Desy Siswanti, S.T., M.T. selaku Pembimbing Akademik.
7. Bapak Ahmad Zarkasih, S.T., M.T. sebagai Ketua Sidang.
8. Bapak Huda Ubaya, S.T., M.T. dan Bapak Sarmayanta Sembiring, S.Si., M.T. sebagai Penguji Sidang.
9. Mbak Renny selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
10. Teman se-SD-SMP-SMA-PTN (Devi Maulitasari), teman seperjuangan Konsentrasi Jaringan yang juga bimbingan dengan Bapak Deris Stiawan dan

Bapak Ahmad Heryanto, kakak-kakak tingkat yang telah memberi arahan dan bantuan serta adik tingkat yang memberi semangat.

11. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2016.
12. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'a.

Penulis menyadari dalam penyusunan laporan Proposal Tugas Akhir ini masih terdapat banyak kekurangan, karenanya penulis mengharapkan kritik dan saran untuk perbaikan. Semoga laporan Proposal Tugas Akhir ini dapat bermanfaat bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Agustus 2020
Penulis

Rahman Ramadhan
NIM. 09011381621082

DDoS UDP Flooding Attack Prevention System with String Matching Method in Real-Time

Rahman Ramadhan (09011381621082)
Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email : rahmanramadhan89@gmail.com

ABSTRACT

Distributed Denial of Service attacks prevents authorized users from accessing the service. One type of DDoS attack is a UDP flood, in which an attacker tries to flood the server traffic by sending a lot of requests with the UDP protocol. In this research, the string matching algorithm was successful in detecting the UDP flood attack by utilizing the payload as a pattern. With the detection result using string matching, then performing the process of taking attributes for blacklisting so that it can be used for the prevention process using an IPTABLES. The detection results using string matching obtained a true positive rate of 83% with a False Positive Rate of 0% and an accuracy of 83%. While the prevention using IPTABLES obtained a True Positive Rate of 100% with a False Positive Rate of 4% and an accuracy of 99%.

Keywords : UDP *flooding, string matching, IPTABLES.*

Sistem Pencegahan Serangan DDoS UDP *Flooding* dengan Metode *String Matching* Secara *Real-Time*

Rahman Ramadhan (09011381621082)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email : rahmanramadhan89@gmail.com

ABSTRAK

Serangan Distributed Denial of Service membuat user yang sah tidak dapat mengakses layanan. Salah satu jenis serangan DDoS adalah UDP flood, di mana penyerang mencoba membanjiri lalu lintas server dengan mengirimkan request dengan protokol UDP dalam jumlah yang banyak. Dalam penelitian ini, algoritma string matching berhasil mendeteksi serangan UDP flood dengan memanfaatkan payload sebagai pola. Hasil dari deteksi menggunakan string matching kemudian dilakukan proses pengambilan atribut untuk pembuatan blacklist sehingga dapat digunakan untuk proses pencegahan menggunakan IPTABLES. Hasil deteksi menggunakan string matching diperoleh nilai *true positive rate* sebesar 83% dengan *False Positive Rate* sebesar 0% dan akurasi sebesar 83%. Sedangkan, hasil pencegahan dengan IPTABLES diperoleh nilai *True Positive Rate* sebesar 100% dengan *False Positive Rate* 4% dan akurasi sebesar 99%.

Kata kunci : UDP *flooding, string matching, IPTABLES.*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I. PENDAHULUAN

1.1. Latar Belakang

Serangan terhadap jaringan internet atau *cyber attack* sudah sering terjadi dan banyak jenisnya, salah satu jenisnya ialah serangan *Distributed Denial of Service* (DDoS). Adapun yang dimaksud dengan serangan DDoS adalah serangan terhadap jaringan internet yang terkoordinasi pada layanan dan *resource* dari internet yang berskala besar [1]. Contoh *resource* tersebut berupa *memori, buffer, bandwidth, CPU*, dan lain lain. Target dari serangan DDoS biasanya *user* atau organisasi yang memiliki hak akses yang sah, yang berdampak akan hilangnya *service* seperti *website*, email dan koneksi internet. Serangan DDoS beroperasi dengan cara menggunakan berbagai *bot* atau *zombie* untuk membuat sumber daya internet penuh oleh paket berskala besar sehingga tidak dapat di akses oleh pengguna yang sah [2]. Berdasarkan hal tersebut perlu dilakukan pencegahan untuk menjaga ketahanan sistem komputer. Maka dari itu, untuk menambahkan atau melakukan aksi pencegahan terhadap serangan, diperlukannya sebuah metode serperti *firewall* yang biasa disebut dengan *Intrusion Prevention System* atau IPS.

Berdasarkan penelitian [3], *Intrusion Prevention System* (IPS) merupakan metode yang sering digunakan untuk menjaga ketahanan komputer dari berbagai serangan *cyber* yang mengkombinasikan metode *Intrusion Detection System* (IDS) dan *firewall* dengan sangat baik. Teknologi IPS memiliki kinerja yang bertujuan untuk mencegah serangan yang masuk melalui *traffic* jaringan dengan cara memeriksa berbagai *log* paket data dan mencegahnya berdasarkan *signature* yang dikenali dari sensor pengenalan pola. IPS akan melakukan *block* atau *drop* pada paket yang teridentifikasi sebagai serangan dan mencatat data yang identik dengan *signature database*. Jadi IPS akan bertindak sebagai layaknya *firewall* yang akan melakukan *allow* atau *block* terhadap paket serangan yang di deteksi oleh mesin IDS. IPS merupakan salah satu cara efektif yang memiliki peran untuk mengenali serangan dari *traffic* jaringan dan mencegah serangan tersebut masuk ke sumber daya [4].

Pada kasus serangan DDoS, banyak peneliti yang telah melakukan eksperimen untuk mendapatkan metode terbaik dalam mendeteksi serangan. Diantaranya penelitian [5] yang membahas tentang deteksi *TCP Flooding attack* dalam lingkungan *cloud*, serta pada penelitian [6] mendeteksi serangan *unknown Dos attack* dengan metode *Artificial Immune System* secara *real-time*. Namun penelitian tersebut hanya sebatas untuk memberikan sebuah *alert*.

Berdasarkan uraian yang telah dijelaskan, pada penelitian ini akan dilakukan suatu penelitian yang berfokus mengenai *intrusion prevention system* DDoS UDP *Flooding* Dengan Metode *String Matching* Secara *Real-Time*. Pada penelitian ini diharapkan dapat melakukan pencegahan terhadap serangan DDoS dan menghasilkan akurasi yang cukup tinggi dalam mendeteksi dan mencegah serangan DDoS secara *Real-time* terutama serangan UDP *Flooding*.

1.2. Tujuan

Adapun tujuan penelitian ini adalah untuk:

1. Mengimplementasikan metode *String Matching* untuk mendeteksi serangan UDP *Flooding*.
2. Melakukan pencegahan dari serangan UDP *Flooding* secara *real-time*.

1.3. Manfaat

Manfaat dalam penelitian ini adalah dapat memberikan tindakan preventif terhadap serangan UDP *Flooding* dengan metode *string matching* secara *real-time*.

1.4. Rumusan Masalah

Berdasarkan permasalahan yang dipaparkan dalam latar belakang diatas, peneliti merumuskan masalah penelitian ini sebagai berikut:

1. Bagaimana mengimplementasikan metode *String Matching* untuk mendeteksi serangan UDP *Flooding*?
2. Bagaimana melakukan pencegahan dari serangan UDP *Flooding* secara *real-time*?

1.5. Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah sebagai berikut:

1. Menggunakan metode *string matching*.
2. Mendeteksi serangan UDP *Flooding*.

1.6. Metodologi Penelitian

Metodologi yang digunakan dalam penulisan Proposal Tugas Akhir akan melalui beberapa tahapan sebagai berikut :

1. Tahap Pertama (Studi Pustaka/Literatur)

Dalam tahap pertama ini penulis mencari masalah yang sesuai dan relevan untuk diangkat sebagai penelitian. Kemudian, penulis mencari beberapa sumber seperti jurnal, buku, artikel dan lain sebagainya yang memiliki keterkaitan dengan tugas akhir.

2. Tahap Kedua (Perancangan *System*)

Pada tahap kedua ini merupakan tahap yang membahas masalah proses merancang sebuah *system*, software dan hardware yang digunakan beserta konfigurasi *system* dan menerapkan *system*.

3. Tahap Ketiga (Pengujian)

Dalam tahap ketiga merupakan tahap dimana penulis melakukan pengujian berdasarkan metodologi penelitian sehingga mendapatkan hasil yang sesuai dan tepat secara konsep atau praktis.

4. Tahap Keempat (Analisa)

Pada tahap keempat, dilakukan analisis data yang telah diperoleh dari hasil pengujian untuk mendapatkan hasil yang objektif berdasarkan pendekatan tertentu.

5. Tahap Kelima (Kesimpulan dan Saran)

Dalam tahap ini akan ditarik suatu kesimpulan yang didapat dari tahapan – tahapan sebelumnya, dan ditambahkan saran untuk dijadikan sebagai landasan untuk penelitian selanjutnya.

1.7. Sistematika Penulisan

Dalam proses penyusunan tugas akhir dan memperjelas isi dari setiap bab maka dibuatlah sistematika penulisan sebagai berikut :

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi lata belakang, tujuan, manfaat, rumusan masalah, dan batasan masalah kemudian metodologi penelitian serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab ini berisi penjelasan teori dari *Intrusion Detection System*, *Intrusion Prevention System*, *Distribution Denial of Service*, *String Matching*, dan teori-teori lain yang berkaitan dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem (*System Design*) dan penerapan metode penelitian.

BAB IV. HASIL DAN ANALISA

Pada bab ini menjelaskan hasil pengujian terhadap sistem yang telah dibangun serta analisis dari data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN

Pada bab ini berisi kesimpulan tentang penelitian yang dilakukan, serta menjawab tujuan yang hendak dicapai pada BAB I (Pendahuluan).

DAFTAR PUSTAKA

[1] H. Chau, “Network Security – Defense Against DoS / DDoS Attacks,” pp. 1–11, 2000.

[2] M. Darshan .L and R. S. Jadon, “Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches,” vol. 7782, no. Layer 7, pp. 183–197, 2014.

[3] D. Stiawan, A. H. Abdullah, and M. Y. Idris, “The trends of Intrusion Prevention System network,” *ICETC 2010 - 2010 2nd Int. Conf. Educ. Technol. Comput.*, 2010.

[4] Y. Farhaoui, “Design and Implementation of an Intrusion Prevention System,” vol. 19, no. May, 2017.

[5] A. Sahi, D. Lai, Y. Li, and M. Diykh, “An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment,” vol. 3536, 2017.

[6] D. Wang, L. He, Y. Xue, and Y. Dong, “EXPLOITING ARTIFICIAL IMMUNE SYSTEMS TO DETECT UNKNOWN DoS ATTACKS IN REAL-TIME,” pp. 1–5, 1857.

[7] M. Yasodha and S. Umarani, “Bandwidth based Distributed Denial of Service Attack Detection using Artificial Immune System,” vol. 2, no. 6, pp. 1–4, 2015.

[8] P. Jokar and V. C. M. Leung, “Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids,” vol. 3053, pp. 1–12, 2016.

[9] M. Poongodi *et al.*, “Intrusion Prevention System for DDoS attack on VANET with reCAPTCHA Controller using Information based metrics,” *IEEE Access*, vol. PP, p. 1, 2019.

[10] J. Lee, J. Woo, and J. An, “Improved Pattern Matching Method for Intrusion Detection Systems under DDoS Attack,” vol. 8, October, 2015.

[11] Y. Chi, “Design and Implementation of Cloud Platform Intrusion Prevention System based on SDN,” pp. 847–852, 2017.

[12] Z. Xu, K. R. Choo, A. Dehghantanha, R. Parizi, and M. Hammoudeh,