DETEKSI SERANGAN DNS AMPLIFICATION MENGGUNAKAN METODE BLOOM FILTER

TUGAS AKHIR

DISUSUN OLEH:

JUANDA FAHRIZAL

09011181520006

UNIVERSITAS SRIWIJAYA

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

2020

HALAMAN PENGESAHAN

DETEKSI SERANGAN DNS AMPLIFIATION MENGGUNAKAN METODE BLOOM FILTER

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

JUANDA FAHRIZAL
09011181520006

Indralaya, Juli 2020

Pembimbing I,

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

Pembimbing II,

Ahmad Heryanto, S.Kom.,M
NIP 198701222015041002

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Pada hari Jumat 13 Maret 2020 telah dilaksanakn ujian sidang tugas akhir oleh Sarjana Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Juanda Fahrizal

NIM : 09011181520006

Judul : Deteksi Serangan DNS Amplification Menggunakan Metode Bloom Filter

Tim Penguji :

1. **Ketua**

   Adi Hermansyah, M.T. (.....06/25/2020.....)

2. **Penguji I**

   Huda Ubaya, M.T. (.....6/24/20 0.....)

3. **Penguji II**

   Sarmayanta Sembiring, M.T. (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Juanda Fahrizal
NIM	: 0901181520006
Jurusan	: Sistem Komputer
Judul	: Deteksi Seragan DNS Amplification Menggunakan Metode Bloom Filter

Hasil Pengecekan Softeare iThenticate/Turnitin: **10 %**

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya 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 dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Juli 2020

Juanda Fahrizal
NIM. 09011181520006

HALAMAN PERSEMBAHAN

" Don't give up when you still have something to give. Nothing is really over until the moment you stop trying" - Brian Dyson

Tugas Akhir ini saya persembahkan untuk :

- ***Kedua Orang tua dan Adik saya***
- ***Dosen Pembimbing dan Penguji***
- ***Sahabat – sahabat saya***
- ***Teman Seperjuangan Sistem Komputer 2015***
- ***Almamaterku***

KATA PENGANTAR

Alhamdulillahhirabbil'alamin Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul "Deteksi Serangan *DNS Amplification* Menggunakan *Bloom Filter*" di susun untuk memenuhi sebagian persyaratan kelulusan untuk memperoleh gelar Sarjana Komputer pada Jurusan Sistem Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis menyadari keterbatasan dan kelemahan yang ada dalam menyelesaikan tesis ini sehingga penulis ingin meyampaikan ucapan terimakasih kepada pihak-pihak yang telah memberikan dukungan, bimbingan dan motivasi kepada penulis untuk menyelasaikan tugas akhir ini, kepada:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga tugas akhir penulisan ini dapat berjalan dengan lancar.
2. Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi dan semanga.
3. Bapak Jaidan Jauhari, S.Pd, M.T. selaku dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., sebagai Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D. dan Bapak Ahmad Heryanto, S.Kom, M.T. selaku pembimbing yang telah meluangkan waktu, bantuan serta saran dan kritiknya dalam penyusunan tugas akhir ini.
6. Dosen-dosen pengajar yang telah memberikan ilmu bermanfaat kepada penulis selama menuntut ilmu di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Mba Winda Kurnia Sari selaku Administrator Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberi kemudahan dalam pengurusan administrasi.
8. Seluruh teman-teman Jurusan Sistem Komputer Angkatan 2015 yang telah membantu dan memberikan semangat pada masa-masa perkuliahan.
9. Semua pihak yang telah memberi dukungan kepada penulis dan tidak bisa disebutkan satu-persatu.

Akhir kata, penulis menyadari bahwa tugas akhir ini masih banyak kekurangan baik dari isi maupun susunan. Semoga tugas akhir ini dapat bermanfaat untuk kita semua.

Indralaya, Juli 2020

Penulis

DETEKSI SERANGAN DNS AMPLIFICATION MENGGUNAKAN METODE BLOOM FILTER

Juanda Fahrizal (09011181520006)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
E-mail : juandafahrizal013@gmail.com

ABSTRAK

Serangan *DNS Amplification* merupakan serangan yang memanfaatkan *Open DNS Server* dimana attacker akan memanipulasi *Query* (permintaan) normal menjadi permintaan palsu,serangan ini akan membanjiri permintaan palsu (*False Query*) dalam jumlah yang sangat banyak dengan tempo yang sangat cepat. Dalam penelitian ini di kelompokkan menjadi 3 jenis dataset sehingga mendapatkan dataset yang bersifat homogen. Selanjutnya dataset tersebut dilakukan *data correction* dengan meekstrasi dataset yang telah di dapatkan dengan membandingan dataset normal dan dataset serangan sehingga didapatkan pola serangan yang digunakan untuk melakukan proses deteksi dengan menggunakan metode *Bloom Filter*. *Bloom Filter* mengelompokkan dataset berdasarkan pola yang telah didapatkan oleh penulis kemudian pola tersebut di *hash* dan di ubah ke dalam bentuk *Bit array* yang berguna untuk pendeteksia seranagn *DNS Amplification* dan penghitungan akurasi. Hasil deteksi menggunakan *Bloom Filter* di peroleh nilai dengan tingkat akurasi 98,90%, TPR 98,90%, TNR 100%, dan FPR 57,73% Bloom Filter tidak menyajikan data *False Negative Rate*.

Kata Kunci : *DNS Amplification Attack, Denial of Service, Bloom Filter*

DETECTION DNS AMPLIFICATION ATTACK WITH BLOOM FILTER METHOD

Juanda Fahrizal (09011181520006)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
E-mail : juandafahrizal013@gmail.com

ABSTRACT

DNS Amplification attack is an attack that utilizes Open DNS Server the attacker will manipulate normal queries to fake requests, this attack will flood a much of fake request in fast tempo. It was grouped into 3 types of datasets so as to get a homogeneous dataset. Tthe dataset is performed data correction by extracting the dataset that has been obtained by comparing the normal dataset and the attack dataset so that an attack pattern is obtained to perform the detection using the Bloom Filter method. Bloom Filter classifies a dataset based on a pattern that has been obtained by the author then the pattern is hashed and converted to a Bit array which is useful for detecting DNS Amplification and calculating accuracy. Detection results using Bloom Filter were obtained with an accuracy rate of 98.90%, TPR 98.90%, TNR 100%, and FPR 57.73% Bloom Filter did not present False Negative Rate data.

Keywords : *DNS Amplification Attack, Denial of Service, Bloom Filter*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I. PENDAHULUAN

1.1. Latar Belakang

Pada penelitian [1] *DNS Amplification* adalah serangan yang membuat penyerang mengirimkan *DNS* request dalam jumlah besar ke server korban . Alamat sumber *DNS* ini dipalsukan menjadi alamat korban, setelah itu penyerang akan membanjiri korban dengan *DNS* respons dalam jumlah besar. Dampak dari *DNS Amplification* yaitu *DNS* respons menjadi jauh lebih besar dari *DNS* request yang membuat server korban melakukan response *DNS* secara serus menerus. *DNS Amplification* sering digunakan untuk melakukan serangan yang sangat besar pada suatu server. *DNS Amplification* membanjiri paket *UDP* secara terus menerus ke alamat server korban dalam bentuk *DNS* response secara besar.

Sedangkan penelitian [2] *DNS Amplification* memanfaatkan *Open DNS Server* dimana penyerang akan memanipulasi Query (Permintaan) normal menjadi permintaan palsu. Dengan adanya *Open DNS Server* ini sangat menarik bagi penyerang untuk memanipulasi *DNS* server untuk tujuan yang berbahaya yang merugikan banya korban. Penyerang mengeksploitasi *Open DNS Server* untuk memaksimalkan penyerangan dengan menyembunyikan alamat IP penyerang dari sumbernya. Selanjutnya dihasilkan berupa response palsu dalam jumlah yang sangat besar sehingga server korban mengalami down.

Bloom Filter adalah struktur data biner acak sederhana yang dapat digunakan secara efisien untuk perkiraan pengujian keanggotaan yang ditetapkan. Pada penelitian[3] mengatakan *Bloom Filter* sangat efisien dalam memilih data dan penggunaannya juga sangat mudah. *Bloom Filter* dapat membedakan mana data serangan *DNS Amplification* dan mana data normal dalm waktu yang efisien. Jumlah elemen memeiliki peranan besar dalam pengalokasian *Bloom Filter* dikarnakan semakin banyak jumlah elemen, maka alokasi memori yang dibutuhkan untuk *Bloom Filter* semakin besar.

Dari beberapa rujukan diatas, penulis bermaksud untuk melakukan penelitian pendeteksian terhadap serangan *DNS Amplification* dengan

menggunakan metode *Bloom Filter* untuk dapat mengenali pola serangan *DNS Amplification* dan membedakannya dengan pola data normal.

1.2 TUJUAN

Adapun tujuan dari penelitian ini adalah:.

1. Mengenali pola serangan *DNS Amplification*
2. Menerapkan metode *Bloom Filter* untuk mendeteksi serangan *DNS Amplification*
3. Mengukur akurasi deteksi serangan *DNS Amplification* dengan membandingkan hasil dari *Snort* dan *Bloom Filter*.

1.3 MANFAAT

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Dapat membedakan response *DNS* biasa dengan response *DNS Amplificaiton*
2. Dapat membedakan paket serangan *DNS Amplification* dengan paket normal.

1.4 Rumusan Masalah

1. Bagaimana cara mendeteksi serangan *DNS Amplification* menggunakan metode *Bloom Filters*?.
2. Bagaimana cara membedakan paket yang termasuk paket serangan *DNS Amplification* dan paket normal menggunakan metode *Bloom Filter*?.

1.5 Batasan Masalah

1. Data pengamatan berfokus pada serangan *DNS Amplification*
2. Data akan dikelompokan dalam dua bagian, yaitu paket data normal dan paket serangan.
3. Metode yang digunakan adalah *Bloom Filter*.
4. Pengujian dilakukan dalam ruang lingkup jaringan lokal Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Pengujian metode tidak dilakukan dalam lalu lintas real time.
6. Tidak diujikan pada lalu lintas jaringan yang terenskripsi.
7. Tidak membahas bagaimana cara pencegahan serangan tersebut.

1.6 Metodologi Penelitian

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

1. Pengumpulan Data

   Metode pengumpulan data yang dilakukan adalah studi pustaka atau literatur. Studi *literature* dilakukan dengan cara mempelajari dan mengumpulkan informasi mengenai penelitian yang akan dilakukan. *Literature* tersebut diperoleh dari jurnal, buku dan *mailing list* agar dapat menunjang metedologi dan pendekatan yang akan diterapkan pada penelitian**.**

2. Pengolahan Data

   Tahap ini ialah membahas mengenai proses yang telah dilakukan dalam penelitian kedalam bentuk tulisan. Pengolahan data dimaksudkan untuk melihat kesesuaian hasil penelitian serta mengevaluasi jalannya sistem berdasarkan batasan masalah dari penelitian

3. Pengujian

   Tahap ini merupakan tahap pengujian metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma.

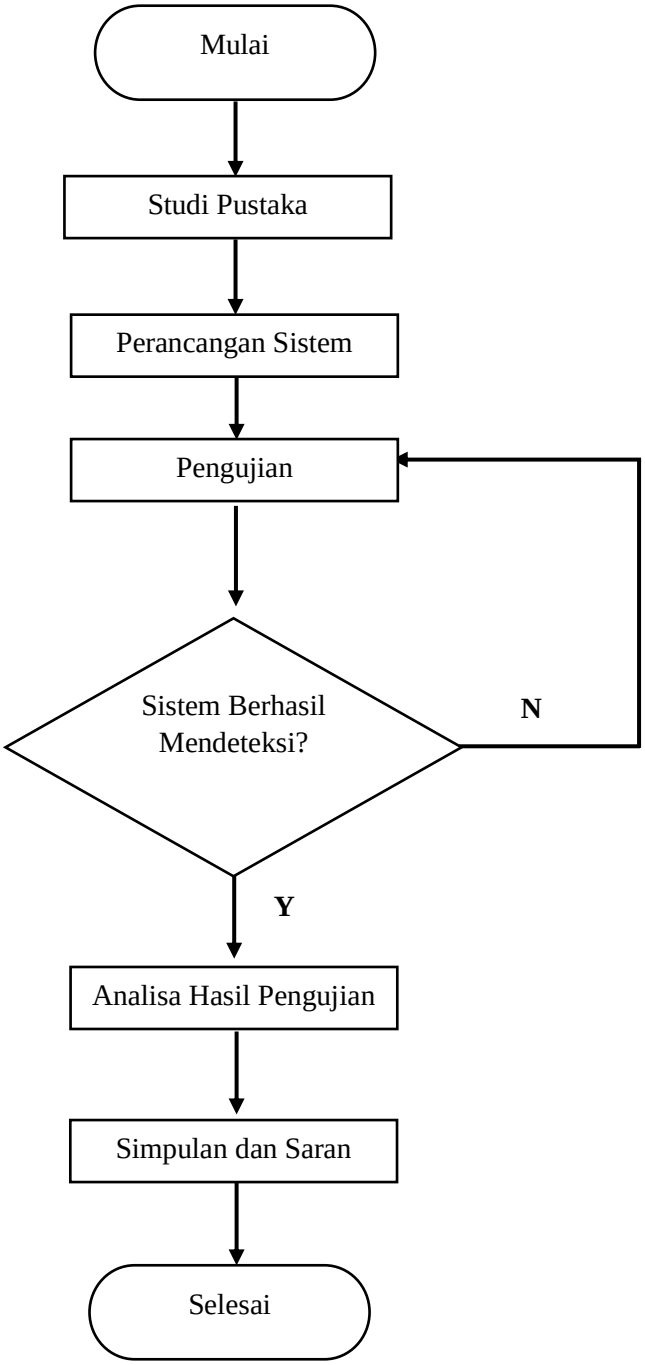
4. Analisa

   Hasil dari pengolahan data pada tahap sebelumnya, akan dianalisa sesuai identifikasi permasalahan. Tahapan ini bertujuan untuk mendapatkan data objektif dari analisa hasil pengolahan data serta dapat dilakukannya pengembangan pada penelitian sebelumnya.

5. Kesimpulan dan Saran

   Pada tahap ini dilakukan penarikan kesimpulan dalam penulisan tugas akhir. Tahapan ini juga terdapat beberapa poin saran dari penulis untuk penelitian selanjutnya

Pada Gambar 1.1 berikut ditampilkan metodologi penelitian secara visual dalam bentuk diagram air yang merepresentasikan proses pelaksanaan penelitian :



Gambar 1.1 Diagram Air Metodologi Penelitian

1.7 Sistematika Penulisan

Penyusunan laporan tugas akhir ini, penulis membuat sistematika penulisan agar mempermudah mengetahui isi dari setiap bab yang dibuat pada laporan tugas akhir ini. Adapun seitematika penulisan laporan tugas akhir sebagai berikut :

BAB I. PENDAHULUAN

Bab ini akan menjelaskan tentang latar belakang masalah, tujuan danmanfaat, perumusan masalah, batasan masalah, metodologi penelitian,serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian terkait dengan *Dns Amplification Attack*, *Intrusion Detection System, Bloom Filter*, dan yang berkaitan langsung dengan penelitian

BAB III. METODELOGI

Bab ini akan menjelaskan tentang langkah-langkah (metodologi) perancangan sistem pada tugas akhir ini..

BAB IV. PENGUJIAN DAN ANALISA

Bab ini akan menjelaskan tentang hasil dari pengujian yang telah dilakukan, dari hasil tersebut akan dilakukan analisa agar mendapatkan data yang akurat.

BAB V. KESIMPULAN

Bab ini akan menjelaskan tentang kesimpulan yang didapat dari data penelitian yang telah dilakukan. Dan saran yang diharapkan dapat membuat penelitian ini dikembangkan lebih baik.

DAFTAR PUSTAKA

[1] V. Gupta and E. Sharma, "Mitigating DNS Amplification Attacks Using a Set of Geographically Distributed SDN Routers," *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 392–400, 2018.

[2] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, "DNS amplification attack revisited," *Comput. Secur.*, vol. 39, no. PART B, pp. 475–485, 2013.

[3] U. Sattar, T. Naqash, M. R. Zafar, K. Razzaq, and F. Bin Ubaid, "Secure DNS from amplification attack by using modified bloom filters," *8th Int. Conf. Digit. Inf. Manag. ICDIM 2013*, pp. 20–23, 2013.

[4] K. Alieyan, M. M. Kadhum, M. Anbar, S. U. Rehman, and N. K. A. Alajmi, "An overview of DDoS attacks based on DNS," *2016 Int. Conf. Inf. Commun. Technol. Converg. ICTC 2016*, pp. 276–280, 2016.

[5] S. S. B and F. Kohnh, "Computer Security – ESORICS 2017," vol. 10493, pp. 437–455, 2017.

[6] P. Panggabean, "Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (Ids) Untuk Optimasi," vol. 6, no. 1, 2018.

[7] A. S. Ashoor and S. Gore, "Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)," *Commun. Comput. Inf. Sci.*, vol. 196 CCIS, pp. 497–501, 2011.

[8] S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi, and S. Ventura, "SIP intrusion detection and prevention: Recommendations and prototype implementation," *1st IEEE Work. VoIP Manag. Secur. VoIP MaSe 2006*, no. May, pp. 45–50, 2006.

[9] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, "Design of a snort-based hybrid intrusion detection system," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5518 LNCS, no. PART 2, pp. 515–522, 2009.

[10] D. V. Sandi and M. Arrofiq, “Implementasi Analisis NIDS Berbasis Snort Dengan Metode Fuzy Untuk Mengatasi Serangan LoRaWAN,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 3, pp. 685–696, 2018.

[11] F. Grandi, “On the analysis of Bloom filters,” *Inf. Process. Lett.*, vol. 129, no. September, pp. 35–39, 2018.

[12] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[13] J. Kim, “On the false positive rate of the bloom filter in case of using multiple hash functions,” *Proc. - 2014 9th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2014*, pp. 26–30, 2014.