DETEKSI SERANGAN UDP *FLOODING* DI *CLOUD COMPUTING* MENGGUNAKAN METODE *SIGNATURE BASED DETECTION*

TUGAS AKHIR

Oleh :

M. Atma Utama Septiando

09011281419052

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

DETEKSI SERANGAN UDP *FLOODING* DI *CLOUD COMPUTING* MENGGUNAKAN METODE *SIGNATURE BASED DETECTION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

M. Atma Utama Septiando

09011281419052

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

HALAMAN PENGESAHAN

DETEKSI SERANGAN UDP *FLOODING* DI *CLOUD COMPUTING* MENGGUNAKAN METODE *SIGNATURE BASED DETECTION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

M. Atma Utama Septiando
09011281419052

Indralaya, Desember 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP. 197806112010121004

Pembimbing

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa
Tanggal : 10 Desember 2019

Tim Penguji :

1. Ketua : **Aditya Putra Perdana, M.T.** (.....)

2. Anggota I : **Dr. Reza Firsandaya Malik, M.T.** (.....)

3. Anggota II : **Sarmayanta Sembiring, M.T.** (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M. Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN KEASLIAN

Nama : **M. Atma Utama Septiando**

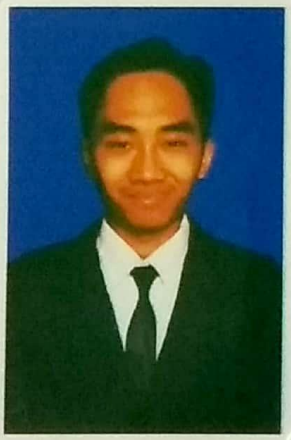
NIM : **09011281419052**

Judul : **Deteksi Serangan UDP *Flooding* di *Cloud Computing* Menggunakan Metode *Signature Based Detection***

Hasil Pengecekan Software i'Ihenticate/Tumitin : 8 %

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 beriaku.

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



Palembang, Desember 2019

METERAI TEMPEL
FCF10AHF146552649
6000
ENAM RIBU RUPIAH

M. Atma Utama S
NIM. 09011281419052

HALAMAN PERSEMBAHAN

وَمَااللَّذَّةُإِلاَّبَعْدَالتَعَبِ

(Tak ada kenikmatan kecuali setelah susah payah)

Skripsi Ini Kupersembahkan Kepada :

Kedua orang tua-ku yang saya sayangi dan saya cintai
(Agus Lukman dan Yenni Rosalina)

Saudara Laki-lakiku
(Harun Al Rasyid)

Saudara Perempuanku
(Eka Sabrina)

Teman-Teman Seperjuangan di Sistem Komputer 2014
(Universitas Sriwijaya)

Semua Kakak Tingkatku (Akt 2011, 2012, 2013)
Serta Semua Adik Tingkatku (Akt 2015, 2016, 2017, 2018, 2019)

Pembimbing Tugas Akhirku
(Deris Stiawan, M.T., PH.D.)

Jurusan Sistem Komputer Fakultas Ilmu Komputer

Almamater Universitas Sriwijaya

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir dengan judul "**Deteksi Serangan UDP *Flooding* di *Cloud Computing* Menggunakan Metode *Signature Based Detection*"**. Shalawat dan salam tak lupa kita junjungkan kepada Nabi kita Rasulullah SAW beserta keluarga, sahabat dan para pengikutnya hingga akhir zaman.

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan bimbingan, pengarahan, dorongan, bantuan baik moril maupun materil selama penyusunan tugas akhir ini dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa sangat bersyukur kepada Allah SWT dan terima kasih kepada yang terhormat :

1. Orang tuaku, Bapak Agus Lukman dan Ibu Yenni Rosalina serta kedua adik saya yang telah memberikan do'a dan dukungannya serta memberikan Motivasi untuk tetap selalu berusaha dan tawakal.
2. Bapak Jaidan Jauhari, S.Pd., M.T., Selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Rossi Passarella, S.T., M.Eng. Selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, M.T., Ph.D. Selaku Pembimbing tunggal Tugas Akhir di Jurusan Sistem Komputer.
5. Bapak Deris Stiawan, M.T., Ph.D. Selaku Pembimbing Akademik di Jurusan Sistem Komputer.
6. Bapak Dr. Reza Firsandaya Malik, M.T. Selaku Penguji I sidang Tugas Akhir di Jurusan Sistem Komputer.
7. Bapak Sarmayanta Sembiring, M.T. Selaku Penguji II sidang Tugas Akhir di Jurusan Sistem Komputer.
8. Bapak Aditya Putra Perdana, M.T. Selaku Ketua Sidang Tugas Akhir di Jurusan Sistem Komputer.

9. Mbak Winda Kim Selaku Admin jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
10. Mbak Oktaria Iis Selaku Staf Admin Akademik di Fakultas Ilmu Komputer yang juga membantu mengurus seluruh berkas.
11. Seluruh Dosen Jurusan Sistem Komputer Fasilkom Universitas Sriwijaya yang telah memberikan motivasi kepada saya selaku penulis Tugas Akhir.
12. Seluruh Staf Fakultas Ilmu Komputer yang sudah bekerja keras khususnya di Jurusan Sistem Komputer.
13. Kakak tingkat yang telah memberikan motivasi dan masukan, Kak Muhammad Fachruroji Ilham Saputra, Kak Bramantio Rizki Nugroho S.Kom, Kak Deni Danuarta S.Kom, Kak Dimas Wahyudi S.Kom.
14. Seluruh teman-teman , kakak tingkat, adik tingkat angkatan 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018 serta 2019 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
15. Teman-teman satu angkatan sekaligus satu grup riset yang telah memberikan masukan dan saran, Fahron S.Kom, Anggit Mardian S.Kom, Ahmad Ridwan S.Kom, Aidil Fitri Ansyah S.Kom, Gonewaje S.Kom, Sigit Wijaya S.Kom, Randa Fratelli S.kom, , Yonatan Riyadhi S.Kom.
16. Teman-teman angkatan sekaligus satu grup kelompok belajar yang telah menyemangati dan memberi masukan, Ageng Setyo Nugroho S.Kom, Andika Atmanegara S.Kom, Galang Pratama, Gilang Pratama, Cristian Prabowo, Rendika, Adit, Anshori, Arifki, Fadli, Ilham.

Penulis menyadari bahwa laporan Tugas Akhir ini masih jauh dari kesempurnaan, oleh karena itu kritik dan saran yang membangun sangat penulis harapkan sebagai bahan acuan dan perbaikan untuk penulis dalam menyempurnakan laporan Tugas Akhir ini.

Semoga laporan tugas akhir ini bisa bermanfaat bagi pembaca ataupun bagi penulis sendiri. Demikian yang bisa penulis sampaikan.

Wassalamu'alaikum Wr.Wb

Indralaya, Desember 2019

M. Atma Utama S

DETEKSI SERANGAN UDP *FLOODING* DI *CLOUD COMPUTING* MENGGUNAKAN METODE *SIGNATURE BASED DETECTION*

M. Atma Utama Septiando (09011281419052)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : muhammadatma10@gmail.com

Abstrak

Suatu peretasan situs web atau layanan web tidak hanya dapat ditujukan ke jaringan biasa tetapi juga bisa ditujukan terhadap komputasi awan. Deteksi merupakan suatu proses melakukan pemeriksaan terhadap sesuatu dengan menggunakan teknik tertentu. Serangan UDP *Flooding* adalah serangan yang dilakukan oleh *hacker* yang bermaksud untuk menghambat aliran data server korbannya dengan cara membanjiri *port* sebuah *remote host* secara acak. *Owncloud X* merupakan perangkat lunak *cloud infrastructure as a service* (IAAS) berbasis penyimpanan dan pada riset ini digunakan *cloud* yang bersifat publik. Riset ini membahas tentang deteksi serangan *UDP Flooding* di *Owncloud* menggunakan metode *Signature Based Detection* yang menghasilkan klasifikasi serangan antara paket serangan dan normal. Hasil klasifikasi tersebut kemudian dievaluasi dengan *confusion matrix* untuk menghitung seberapa besar tingkat akurasi dari deteksi paket serangan dan normal menggunakan *Signature Based Detection*. Dari riset ini diperoleh tingkat akurasi sebesar 99% dimana perolehan ini ialah hasil akurasi yang sangat baik.

Kata Kunci : Deteksi, UDP *Flooding*, *Cloud Computing*, *Snort* IDS, *Signature Based Detecion*

DETECTION OF UDP FLOODING ATTACKS IN CLOUD COMPUTING USING THE SIGNATURE BASED DETECTION METHOD

M. Atma Utama Septiando (09011281419052)
Dept of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : muhammadatma10@gmail.com

ABSTRACT

A website or web service hacking can not only be addressed to a regular network but can also be addressed to cloud computing. Detection is a process of examining something using a particular technique. UDP Flooding attacks is an attack performed by hackers who intend to inhibit the flow of data on the victim's server by flooding the ports of a remote host randomly. Owncloud X is a cloud software in infrastructure as a service (IAAS) storage based and in this research is used cloud that is public. This research discusses the detection of UDP Flooding attacks in Owncloud using the Signature Based Detection method which generates classification of attacks between the attack and normal packets. The classification result is then evaluated with confusion matrix to calculate accuracy level of the attack packet detection and normal packet using Signature Based Detection. From this research gained an accuracy rate of 99% where this acquisition is an excellent result of accuracy.

Keyword : *Detection, UDP Flooding, Cloud Computing, Snort IDS, Signature Based Detecion*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

User Datagram Protocol (UDP) adalah protokol *sessionless/ connectionless* yang digunakan untuk operasi IP, diagnostik, dan kesalahan. Serangan UDP *Flooding* bisa dikatakan sebagai serangan DDOS ataupun DOS. Serangan UDP *Flooding* dikatakan DDOS adalah jika serangan tersebut dilakukan oleh lebih dari satu komputer tetapi bisa juga dikatakan sebagai serangan DOS jika dilakukan oleh satu komputer. UDP *Flooding* yang dilakukan dengan cara pengiriman sejumlah besar paket UDP ke *random port* pada host dalam range yang jauh. Pada sebagian besar kasus, penyerang memalsukan *IP SRC* yang mudah dilakukan karena protokol UDP "tanpa koneksi" dan tidak memiliki jenis mekanisme apa pun. Serangan ini bertujuan untuk menjenuhkan pipa Internet. Serangan ini juga berdampak pada jaringan dan elemen keamanan dalam perjalanan ke *server* target, dan sebagian besar *firewall. Firewall* membuka keadaan untuk setiap paket UDP dan akan kewalahan oleh koneksi *flooding* dengan sangat cepat [1].

Pada survey berikut [1], membahas persoalan keamanan pada *cloud computing.* Survey tersebut menghasilkan pernyataan bahwa keamanan di lingkungan *Cloud* adalah prioritas utama. Dan itu masih banyak harus diperbaiki mengingat kemajuan teknologi dan jaman yang juga memungkinkan para penjahat *cyber* semakin pintar untuk berbuat kejahatan di dunia maya termasuk di lingkungan *Cloud.*

Pada penelitian selanjutnya [3], *Secret/Encription, integrity, availability, accountability* dan *privacy* adalah nilai nilai terpenting yang dibahas dalam keamanan *cloud computing.*

Penelitian berikutnya [4], yakni membahas tentang kerentanan yang ada pada *cloud* dan tipe serangan yang terjadi pada *cloud* serta taksonomi dari keamanan *cloud* computing juga dibahas pada penelitian ini. Penelitian ini

menyatakan bahwa hal yang cukup penting pada *cloud* adalah mengidentifikasi serangan di lingkungan *cloud computing*.

Terjadi kasus serangan pada *cloud computing* pada bulan Juli 2012 dimana kelompok hacker "UGNazi" meretas sistem *gmail* dan sistem *voicemail AT&T*. Kemudian kelompok tersebut berhasil mendapatkan akses pada akun gmail CEO dari *CloudDare*. Serangan ini pun terjadi pada penyedia layanan *cloud dropbox* pada bulan Juli 2012 dimana peretas mencuri file email dan password dari dropbox user.

Di dalam pembahasan ini, *cloud* menjadi target serangan *UDP Flooding* yang kemudian akan dilakukan pendeteksian serangan tersebut menggunakan metode *signature base*. Pada metode ini sebenarnya terbagi menjadi 3 cara penyelesaian yaitu *Deep Packet Inspection* (DPI), *Stateful Packet Inspection* (SPI), *dan Regular Expression (*RegEx). Dan disini penulis memilih cara penyelesaian dengan menggunakan RegEx.

1.2 Tujuan

Antara lain tujuan pembahasan ini ialah sebagai berikut :

1. Melakukan ekstraksi fitur paket serangan UDP *Flooding* dan paket normal serta membandingkan dengan hasil *capture* paket data *Wireshark.*
2. Menerapkan metode *signature base* untuk menganalisa serangan tersebut (yang terjadi di *cloud*).
3. Menganalisis kerentanan *cloud* pada serangan UDP *Flooding*.
4. Mendeteksi serangan-serangan UDP *Flooding* yang terjadi pada *Cloud Computing*.

1.3 Manfaat

Dibawah ini yakni manfaat yang bisa diarnbil dari riset ini :

1. Mampu menjelaskan penggunaan *string matching* RegEx untuk melacak serangan-serangan yang dilakukan *attacker* UDP.
2. Mendeteksi serangan UDP *Flooding* yang terjadi pada *cloud*.

1.4 Perumusan dan Batasan Masalah

Sesuai latar blakang yang tlah diterangkan, jadi rumusan dan batasan masalah yang dituangkan di dalam riset ini ialah :

1.4.1 Perumusan Masalah

1. Bagaimana penyerang dapat melancarkan serangan ke *cloud computing* ?
2. Bagaimana mendeteksi serangan UDP *Flooding* terhadap *cloud computing* ?
3. Di dalam kasus ini, apa saja analisa dari metode *signature base* yang diterapkan ?

1.4.2 Batasan Masalah

1. Pembahasan ini diterapkan di komputasi awan yang umum.
2. UDP *Flooding* hanya berjenis *Denial of Service* (DOS).
3. Serangan UDP *Flooding* dilakukan pada API OCS pada *cloud.*
4. Cara untuk mencegah serangan ini tidak diterangkan dalam penelitian ini.
5. Serangan ini tidak dilakukan secara *real time.*
6. *Signature base* adalah metode yang dijalankan untuk mendeteksi serangan yang kemudian dianalisa.
7. *Dataset* yang dipakai diambil dari *cloud server*.
8. Dalam membuktikan *alert* adanya serangan pada *cloud*, maka dijalankan sistem *snort*.

1.5 Metodologi Penulisan

Ada beberapa fase yang akan dilalui metodologi penulisan tugas akhir, beberapa fase tersebut yaitu :

1. Fase kesatu (Perumusan Masalah)

Fase ini adalah fase untuk memastikan masalah yang *cloud computing* miliki yang sudah dijelaskan pada kajian sebelumnya yakni mendeteksi serangan yang terjadi pada *cloud computing*.

2. Fase kedua (*Literature Review/* Tinjauan Pustaka)

Fase ini merupakan fase mencari sumber pustaka-pustaka ilmiah yang berkaitan dengan topik laporan tugas akhir untuk menguatkan pembahasan yang sedang dilakukan.

3. Fase ketiga (Perancangan/ Metodologi)

Berikutnya merupakan fase metodologi *system* yang akan dibentuk hingga cocok dengan rumusan masalah. Di dalam fase ini dilakukan pemasangan *operational system*, membuat topologi jaringan *cloud* dan mengkonfigurasi *cloud* trsebut.

4. Fase keempat (*Testing*/ Pengujian)

Kemudian pada fase ini, system yang telah dirancang akan dilakukan pengujian. Di dalam fase ini, serangan yang akan diuji terhadap komputasi awan yang sudah dibangun adalah UDP *Flooding* memakai tools *Low Orbit Ion Canon* (LOIC).

5. Fase kelima (Analisa)

Lalu setelah hasil pengujian tersebut didapatkan maka akan dianalisa pada fase ini. Pada fase ini akan dilakukan analisa dari data hasil uji seperti mengukur akurasi, presisi dan *false alarm rate*.

6. Kesimpulan yang disertakan Saran

Di dalam fase ini, kesimpulan dari hasil uji dan analisa pembahasan akan dituangkan serta memberikan beberapa saran untuk acuan referensis jika riset ini ingin diteruskan.

1.6 Sistematika Penulisan

Agar penelitian lebih sistematis dan spesifik maka penyusunan laporan tugas akhir ini terdiri dari berberapa bagian/bab dengan rincian sbb :

BAB I. PENDAHULUAN

Pada bab satu ini terdiri dari penjelasan dengan cara sistematik mengenai topick riset yang diarnbil rneliputi latar belakng, tujuan dan manfaat, batasan dan perumusan masalah, metodelogi dan sistematiika penulisan.

BAB II. TINJAUAN PUSTAKA

Di dalam bab dua ini beriskan tentang teori dasar dari riset yang berkaitan mengenai UDP *Flooding Attack*, komputasi awan, Jaringan dan Keamanan Jaringan, *Signature Based Method*, juga *Snort*. Dan nantinya bab dua ini menjadi acuan atau landasan dalarn menganalisa batas rnasalah yang sudah dijabarkan di dalam bagian sebelumnnya.

BAB III. METODOLOGI

Kemudian pada bab tiga ini berisi penerangan secara bertahap tentang proses penelitian yang dillakukan. Penjabaran terssebut mengenai fase-fase perancangan system serta fase penerpan metodelogi riset.

BAB IV. PENGUJIAN DAN ANALISA

Lalu pada bab empat ini membahas tentang hasil pengujian dataset dimana dataset tersebut tlah dikerjakan saat pengerjaan tugas akhir. Hasilnya kemudian nanti dianalisa dari UDP *Flooding attack* yang dikerjakan terhadap *cloud.*

BAB V. KESIMPULAN DAN SARAN

Kemudian pada bab terakhir ini berisikan konklusi akhir dari pembahasan *research* yang tlah dikerjakan. Serta ada pemberian saran yang dibutuhkan untuk pengembangan riset selanjutnya agar riset menjadi lebih menarik.

DAFTAR PUSTAKA

[1] https://security.radware.com/ddos-knowledge-center/ddospedia/udp-flood/. [Diakses 12 Jan 2018].

[2] D. a. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, “Security issues in cloud environments: A survey,” *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, 2014.

[3] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” *Inf. Sci. (Ny).*, vol. 305, pp. 357–383, 2015.

[4] S. Iqbal *et al.*, “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, 2016.

[5] T. G. Peter Mell, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology,* September 2011.

[6] R. Greiner, "Robert Greiner," 2014. [Online]. Available: http://robertgreiner.com/2014/03/windows-azure-iaas-paas-saas-overview/. [Diakses 5 Feb 2018].

[7] G. M. Wandhare, P. S. N. Gujar, and V. M. Thakare, “Research Article Network Intrusion Detection Technique for Regular Expression Detection Using Dpi in Ad-Hoc,” 2015.

[8] C. C. Yang, C. M. Cheng, and S. D. E. Wang, “Two-phase pattern matching for regular expressions in intrusion detection systems,” *J. Inf. Sci. Eng.*, vol. 26, no. 5, pp. 1563–1582, 2010.

[9] S. Y. Wu and E. Yen, “Data mining-based intrusion detectors,” *Expert Syst. Appl.*, vol. 36, no. 3 PART 1, pp. 5605–5612, 2009.

[10] M. O. F. Engineering, “Deep Packet Inspection using Snort Supervisory Committee Deep Packet Inspection using Snort,” 2016.

[11] https://jalantikus.com/tips/software-hacker-untuk-serangan-ddos/. [Diakses 16 Des 2019].