DETEKSI *SMURF DDOS* PADA JARINGAN *SOFTWARE DEFINED NETWORK* MENGGUNAKAN METODE *NAÏVE BAYES*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

SYUKRAN RIZKI

09011181520019

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

LEMBAR PENGESAHAN

DETEKSI *SMURF DDOS* PADA JARINGAN *SOFTWARE DEFINED NETWORK* MENGGUNAKAN METODE *NAÏVE BAYES*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

SYUKRAN RIZKI
09011181520019

Indralaya, Desember 2019

Pembimbing I

Deris Stiawan, Ph.D
NIP.197806172006041002

Pembimbing II

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

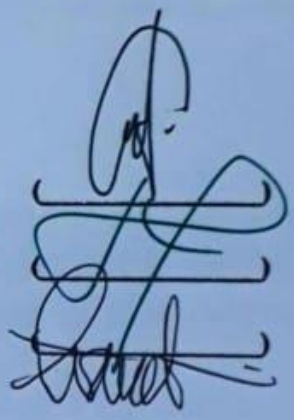
Hari : Sabtu
Tanggal : 21 Desember 2019

Tim Penguji :

1. Ketua : Ahmad Zarkasi, M.T

2. Anggota I : Huda Hubaya, M.T.

3. Anggota II : Tri Wanda Septian, M.Sc.



Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng
NIP 197806112010121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Syukran Rizki

NIM : 09011181520019

Judul TA : Deteksi *Smurf DDoS* pada jaringan *Software Defined Network* menggunakan metode *Naive Bayes*

Hasil Pengecekan *Software iThenticate/Turnitin*: 3%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil plagiat. Apabila ditemukan unsur 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.

Indralaya, Desember 2019

Syukran Rizki

HALAMAN PERSEMBAHAN

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيمِ

"Bersama kesulitan pasti ada kemudahan"

"Sesuatu yang sulit didapatkan akan terasa indah ketika berhasil didapatkan"

"Tidak boleh berhenti berusaha meskipun lelah"

"Titik putus asa letaknya ada di dekat kesuksesan, ketika kamu putus asa berarti kamu menyia-nyiakan kesempatan sukses yang sudah di depan mata"

"Berusaha dan berjuanglah dengan *passion*"

"Belajar itu tidak harus di kelas, tapi juga di rumah, di pasar, di jalan, bahkan saat akan tidur pun kamu harus belajar bagaimana cara tidur yang benar. Belajarhlah atas apapun yang terjadi padamu"

Karya Besar ini kupersembahkan kepada :

- **Kedua orang tua ku yang aku sayangi dan aku cintai.**
  (Syamsul Anwar dan Herlina Syam)
- **Saudara laki-laki kandungku (Randa Ferdiansyah) dan Saudara Perempuan kandungku (Ratih Maharani, Alm. Fatimah).**
- **Keluarga Besar Sistem Komputer.**
- **Teman-teman seperjuangan Sistem Komputer Angkatan 2015.**
- **Almamaterku.**

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT atas berkat rahmat, hidayah, maupun nikmat yg diberikannya berupa kesehatan, pikiran, serta rezeki yang cukup, akhirnya penulisan Tugas Akhir yang berjudul "**Deteksi *Smurf DDoS* pada jaringan *Software Defined Network* menggunakan metode *Naive Bayes***" dapat diselesaikan dengan baik.

Penulis berharap tulisan ini dapat bermanfaat bagi perkembangan ilmu pengetahuan khususnya pada bidang ilmu komputer, semoga tulisan ini dapat menjadi bahan bacaan dan acuan bagi yang tertarik meneliti di bidang jaringan computer khususnya konsentrasi *network security* yang saat ini semakin terus berkembang dan harus selalu dikembangkan untuk mengatasi masalah jaringan komputer.

Penulis sadar bahwa ada banyak kekurangan dalam tulisan yang akan ditemui pembaca di bagian bab inti. Oleh karena itulah kritik dan saran dari pembaca diharapkan dapat membantu memperbaiki di kemudian hari. Semoga peneliti selanjutnya dapat mengambil yang benar dari tulisan ini kemudian memperbaiki yang salah dari isi tulisan ini, sehingga akan menciptakan analisis yang lebih baik lagi.

Penulis tidak lupa mengucapkan terima kasih yang tak terhingga kepada semua pihak yang terlibat pada proses panjang penulisan tugas akhir ini. Mohon maaf jika tidak bisa diucapkan satu per satu secara lengkap di halaman ini, namun semoga yang tertulis dapat mewakili ribuan terima kasih dari penulis. Semoga Allah SWT membalas semua kebaikan dengan lebih banyak kebaikan. Terima kasih atas semua bantuan pikiran, materi, doa, ataupun semangat yang terus mengalir selama proses pembuatan tulisan ini. Ucapan terimakasih penulis dikhususkan kepada :

1. Kepada kedua orang tua saya Syamsul Anwar dan Herlina Syam, yang selalu mendoakan, menjadi inspirasi, serta memberikan motivasi kepada penulis dalam menyelesaikan tugas akhir ini.
2. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Rossi Passarella, M.Eng selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya dan
4. Dosen Pembimbing Akademik bapak Reza Firsandaya Malik, M.T.

5. Bapak Deris Stiawan, Ph.D. selaku Dosen Pembimbing 1 Tugas Akhir dan bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing 2 Tugas Akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan tugas akhir ini.
6. Bapak Huda Hubaya, M.T. dan Tri Wanda Septian, M.Sc. selaku Dosen Penguji sidang Tugas Akhir yang telah memberi banyak masukan berupa kritik dan saran serta ilmu yang bermanfaat sehingga tulisan ini bisa lebih baik.
7. Seluruh Dosen Jurusan Sistem Komputer Fasilkom Unsri.
8. Mbak Winda selaku staf administrasi jurusan Sistem Komputer yang telah sabar dan banyak membantu dalam penyelesaian proses administrasi.
9. Seluruh Staf Pegawai Fakultas Ilmu Komputer Universitas Sriwijaya terutama Staff pegawai di laboratorium mbak widia dan kak cokro.
10. Kepada Adikku Ratih Maharani dan Abangku Randa Ferdiansyah yang telah menjadi penyemangat penulis dalam tugas akhir ini.
11. Kepada kak Anggit Mardian, S.Kom, kak Epriyadi, S.Kom, kak Rendhika Adha Tanjung, S.Kom yang telah membantu dan memberi motivasi kepada penulis.
12. Bangun Sudrajat, Juanda Fahrizal, Ridho Ilham R., yang merupakan teman-teman seperjuangan riset di Laboratorium, dan teman nginap lab yang telah membantu saat proses penyelesaian tugas akhir dan motivasinya.
13. Wulandari Saputri merupakan orang selalu memberi semangat dan motivasi, dalam menyelesaikan tugas akhir ini.
14. Aldo Sapriansyah, Ilham Junius, M. Kadapi, Novit Hardianto, Anggi Tias Kurniawan, Azwar Hidayat, S.Kom, M. Ajran Saputra, S.Kom, yang merupakan teman seperjuangan dan sering memotivasi, memberikan solusi sehingga cukup membantu menyelesaikan tugas akhir ini.
15. Teman seperjuangan di ormawa HIMASISKO Fasilkom Unsri, NAC Fasilkom Unsri, COMNETS RESEARCH GROUP dan lainnya.
16. Serta semua pihak yang telah membantu yang tidak dapat saya sebutkan satu persatu dalam penyelesaian tugas akhir ini, Terima Kasih Semuanya.

Semoga dengan terselesainya tugas akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua. Dalam Penulisan laporan ini penulis juga sangat menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu

penulis mohon saran dan kritik yang membangun untuk Perbaikan Laporan Tugas Akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Palembang, Desember 2019

Penulis

DAFTAR ISI

Daftar Gambar

Daftar Tabel

BAB I. PENDAHULUAN

1.1. Latar Belakang

Pada penelitian [1] Salah satu metode serangan yang dapat digunakan untuk menyerang *controller* SDN adalah serangan *DDoS*. Serangan *DDoS* juga memiliki banyak metode untuk membanjiri sumber daya *controller*. Misalnya, *SYN Flood* dan *ICMP Flood*. Secara umum, serangan *DDoS* mengirimkan sejumlah besar paket dalam waktu tertentu. Di penelitian [1] sedang mengembangkan metode untuk deteksi dan mitigasi serangan *DDoS* di Pengendali SDN. Di penelitian ini menunjukkan potensi dari kerentanan operasi Pengendali SDN yang dapat dieksploitasi untuk serangan *DDoS*.

Dalam penelitian [2] serangan *DDoS* dapat diklasifikasikan dalam berbagai jenis. Salah satu jenis serangan *DDoS* adalah serangan amplifikasi yang dimana *attacker* melakukan pengiriman paket data dalam jumlah besar terhadap computer korban. *Smurf* adalah contoh dari serangan *DDoS* amplifikasi. Jenis serangan ini sebenarnya mengeksploitasi jaringan lain yang tidak dilindungi yang disebut jaringan perantara untuk memperkuat beban lalu lintas serangan yang sebenarnya dikirim ke komputer korban.

Penelitian [3] membahas mengenai deteksi serangan *DoS, Probe, R2L,* dan *U2R* pada jaringan SDN (*Software Defined Network*) kemudian data serangan tersebut diklasifikasi dan dideteksi dengan menggunakan tiga metode algoritma *SVM, J48,* dan *Naïve Bayes.* Pada penelitian ini metode *Naïve Bayes* dapat mengklasifikasi dan mendeteksi serangan dengan akurasi mencapai 95.11%.

Berdasarkan uraian diatas penulis bermaksud untuk melakukan penelitian pendeteksian *Smurf Attack* yang termasuk dalam serangan *Denial Of Service (DoS)* didistribusikan (*DDoS*) pada jaringan *Software Defined Network (SDN)* dengan menggunakan metode *Naive Bayes.*

1.2. Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Membangun jaringan *Software Defined Network (SDN)* berbasis simulasi menggunakan *Mininet*.
2. Mengenali pola serangan *Smurf DDoS.*
3. Menerapkan metode *Naïve Bayes* untuk deteksi serangan *Smurf DDoS.*

4. Melakukan pengukuran akurasi deteksi pada serangan *Smurf DDoS* dengan membandingkan hasil dari *Snort* dan *Naïve Bayes.*

1.3. Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Dapat membedakan arsitektur jaringan *Software Defined Network* dan arsitektur jaringan Tradisional.
2. Dapat mengenali pola serangan *Smurf DDoS*.
3. Dapat mengenali dan membedakan pola trafik normal dengan pola trafik serangan *Smurf DDoS* di jaringan *SDN*.

1.4. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka didapatkan perumusan masalah berikut :

1. Bagaimana merancang jaringan *SDN* berdasarkan sistem simulasi menggunakan *Mininet*?
2. Bagaimana mendeteksi menggunakan metode *Naïve Bayes* pada serangan *Smurf DDoS*?
3. Bagaimana cara membandingkan hasil akurasi yang di dapat dari *Snort* dan metode *Naïve Bayes?*

1.5. Batasan Masalah

Berdasarkan rumusan masalah diatas, maka batasan masalah yang dapat diambil pada tugas akhir ini antara lain :

1. Data serangan yang digunakan pada penelitian ini berfokus pada serangan *Smurf DDoS.*
2. Metode yang digunakan untuk mendeteksi menggunakan metode *Naïve Bayes*.
3. Menjalankan jaringan *Software Defined Network* menggunakan simulasi *Mininet* dan *Controller* menggunakan *POX*.
4. Penelitian ini tidak membahas cara pencegahan pada serangan tersebut.
5. Penelitian ini tidak dilakukan pada lalu lintas jaringan yang terenkripsi.

1.6. Metodologi Penelitian

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

1. Studi Pustaka/Literatur

Pada tahapan ini setelah mengetahui masalah dan sumbernya dijadikan sebagai penelitian kemudian membaca jurnal atau makalah yang terkait dengan tugas akhir ini.

2. Perancangan sistem

Pada tahap ini menguraikan langkah-langkah dalam merancang sistem dengan sistematis menggunakan metode yang telah ditentukan. Lalu menentukan perangkat keras yang digunakan, kemudian perangkat lunak, bahasa pemrograman dan jaringan yang akan digunakan dalam merancang sistem tersebut. Setelah itu melakukan deteksi serangan menggunakan algoritma dengan metode *Naïve Bayes*.

3. Pengujian

Tahap ini membahas pengujian yang akan dilakukan berdasarkan dengan metodologi penelitian telah ditentukan, kemudian didapatlah hasil uji yang sesuai dengan batasan masalah dan parameter yang telah ditentukan sebelumnya.

4. Pengujian

Pada tahap ini dilakukan analisa hasil pengujian untuk mengetahui kekurangan dan faktor penyebabnya sehingga dapat diperbaiki dan dapat dilakukan pengembangan pada penelitian selanjutnya.

5. Kesimpulan dan Saran

Pada tahap ini dilakukan dapat memberi kesimpulan dari analisa dan studi literature serta saran untuk penulis selanjutnya yang kemudian dapat dijadikan bahan referensi untuk penelitian selanjutnya.

1.7. Sistematika Penelitian

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari tiap bab, maka dibuat suatu sistematika penulisan sebagai berikut :

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah dan Batasan Masalah kemudian Metodologi Penelitian, dan yang terakhir mengenai Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian terkait dengan *Software Defined Network, Intrusion Detection System, Distributed Denial Of Service*, *Naïve Bayes*, dan yang berkaitan langsung dengan penelitian

BAB III. METODOLOGI PENELITIAN

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

BAB IV. PENGUJIAN DAN ANALISISA

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN

Bab ini berisi kesimpulan tentang penelitian yang dilakukan, serta menjawab setiap tujuan yang hendak dicapai sesuai yang tercantum pada BAB I (Pendahuluan).

Daftar Pustaka

[1] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, "Time-based DDoS detection and mitigation for SDN controller," *17th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a Very Connect. World, APNOMS 2015*, pp. 550–553, 2015.

[2] S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) attack amplification in internet," *Second Int. Conf. Internet Monit. Prot. ICIMP 2007*, no. 0521585, 2007.

[3] A. Alshamrani, A. Chowdhary, S. Pisharody, D. Lu, and D. Huang, "A defense system for defeating DDoS attacks in SDN based networks," *MobiWac 2017 - Proc. 15th ACM Int. Symp. Mobil. Manag. Wirel. Access, Co-located with MSWiM 2017*, no. November, pp. 83–92, 2017.

[4] S. M. S. Mousavi and M. St-Hilaire, "Early Detection of DDoS Attacks in Software Defined Networks Controller*2014*," , pp. 77–81, 2014.

[5] A. Shalimov, D. Zimarina, and V. Pashkov, "Advanced Study of SDN / OpenFlow controllers," *Cee-Secr '13*, pp. 1–6, 2013.

[6] X. Zhu, Y. Yu, H. Wang, and B. Zeng, "Intrusion detection system model based on extension detecting," *2007 Int. Conf. Converg. Inf. Technol. ICCIT 2007*, pp. 1536–1540, 2007.

[7] D. J. Brown, B. Suckow, and T. Wang, "A Survey of Intrusion Detection Systems 2 Information Sources Analysis Techniques."

[8] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, "Design of a Snort-Based Hybrid Intrusion Detection System," vol. 5518, no. June 2009, 2009.

[9] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: A classification," *Proc. 3rd IEEE Int. Symp. Signal Process. Inf. Technol. ISSPIT 2003*, pp. 190–193, 2003.

[10] A. Prasetyo, L. Affandi, and D. Arpandi, "Implementasi metode naive bayes untuk intrusion detection system (ids)," *J. Inform. Polinema*, vol. 4, pp. 280–284, 2018.

[11] A. Pattekari, S.A.; Parveen, "Prediction system for heart disease using Naïve Bayes," *Int. J. Adv. Comput. Math. Sci.*, vol. 3, no. 3, pp. 290–294, 2012.

[12] N. Ben Amor, S. Benferhat, and Z. Elouedi, "Naive Bayes vs decision trees in intrusion

detection systems," p. 420, 2004.

[13] Bustami, "Penerapan Algoritma Naive Bayes Untuk Mengklasifikasi Data Nasabah Asuransi," *J. Inform.*, vol. 8, no. 1, 2014.

[14] S. R. Afif, P. Sukarno, and M. A. Nugroho, "Analisis Perbandingan Algoritma Naive Bayes dan Decision Tree untuk Deteksi Serangan Denial of Service (DoS) pada Arsitektur Software Defined Network (SDN) Pendahuluan Studi Terkait," *e-Proceeding Eng.*, vol. 5, no. 3, pp. 7515–7521, 2018.

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