IMPLEMENTASI ALGORITMA CM-SPADE DALAM MEMBANGUN MODEL SISTEM DETEKSI *DENIAL OF SERVICE* MENGGUNAKAN SNORT

SKRIPSI

diajukan untuk memenuhi sebagian dari
persyaratan untuk memperoleh gelar Sarjana Ilmu Komputer
pada Departemen Pendidikan Ilmu Komputer
Program Studi Pendidikan Ilmu Komputer

Oleh:

Samekto Rinekso Pribadi

NIM 1202329

PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA

2019

IMPLEMENTASI ALGORITMA CM-SPADE DALAM MEMBANGUN MODEL SISTEM DETEKSI *DENIAL OF SERVICE* MENGGUNAKAN SNORT

Oleh

Samekto Rinekso Pribadi

NIM 1202329

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2019

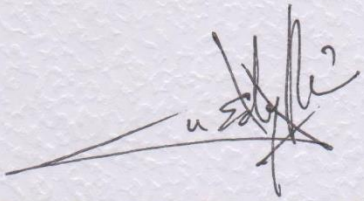
LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA CM-SPADE DALAM MEMBANGUN MODEL SISTEM DETEKSI DENIAL OF SERVICE MENGGUNAKAN SNORT

Oleh:

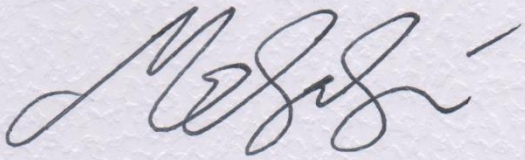
Samekto Rinekso Pribadi
NIM 1202329

DISETUJUI DAN DISAHKAN OLEH:
Pembimbing I,



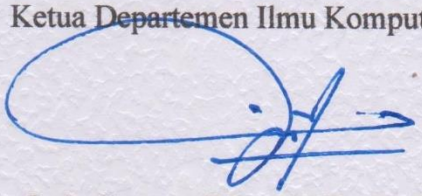
Eddy Prasetyo Nugroho, M.T.
NIP 197505152008011014

Pembimbing II,



Dr. Rani Megasari, M.T.
NIP 198705242014042002

Mengetahui,
Ketua Departemen Ilmu Komputer



Lala Septem Riza, M.T., Ph.D
NIP 197811262008121001

PERNYATAAN

Saya menyatakan bahwa skripsi yang berjudul "**Implementasi Algoritma CM-SPADE dalam Membangun Model Sistem Deteksi *Denial of Service* Menggunakan Snort**" ini sepenuhnya merupakan karya sendiri. Tidak ada plagiat dari orang lain di dalamnya dan saya tidak melakukan penyalinan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung saksi yang dijatuhkan kepada saya apabila ditemukan adanya pelanggaran terhadap etik dan keilmuan di karya ini atau ada klaim dari pihak lain terhadap keaslian karya ini.

Bandung, Agustus 2019

Pembuat pernyataan,

Samekto Rinekso Pribadi

1202329

KATA PENGANTAR

Segala puji bagi Allah SWT atas kehendak dan izin-Nya-lah penulis dapat menyelesaikan skripsi yang berjudul "**Implementasi Algoritma CM-SPADE dalam Membangun Model Sistem Deteksi *Denial of Service* Menggunakan Snort**" dengan sebaik-baiknya dan dalam waktu tepat. Shalawat serta salam semoga senantiasa tercurah limpah kepada makhluk utusan Allah Rasulullah, Nabiallah, Muhammad SAW kepada keluarga, sahabat, tabi'in, dan sampai kepada kita sebagai pengikutnya.

Penulisan skripsi ini ditunjukkan untuk menempuh dan melengkapi salah satu syarat untuk mendapatkan gelar Sarjana Komputer pada Jurusan Program Studi Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia (FPMIPA UPI).

Akhir kata penulis sampaikan permohonan maaf atas segala kesalahan dalam skripsi ini. Penulis mengharapkan kritik dan saran yang membangun dari pembaca. Semoga skripsi ini dapat bermanfaat bagi kalangan akademis, khususnya bagi mahasiswa ilmu komputer, masyarakat pada umumnya, dan bagi dunia ilmu pengetahuan.

Bandung, Agustus 2019

Penulis,

Samekto Rinekso Pribadi

1202329

UCAPAN TERIMA KASIH

Selama proses penyelesaian skripsi ini tentunya tidak lepas dari berbagai kendala dan hambatan. Namun dibalik itu semua, ada dukungan dan dorongan dari berbagai pihak disekitar lingkungan penulis yang tiada lelah mengingatkan, memotivasi, membantu, serta dukungan baik moril atau materil. Oleh karena itu, pada kesempatan ini saya selaku penulis buku skripsi ini ingin menyampaikan ucapan terima kasih yang sebesar-besarnya serta penghargaan kepada:

1. Allah SWT, karena tanpa rahmat, karunia dan ridha-Nya tidak akan ada yang bisa penulis capai walaupun berusaha sekeras mungkin
2. Kepada orang tua saya tercinta, Ibu Anna Ratnasari Dewi dan Bapak Sukowiyono yang telah bersabar dan selalu memberikan dukungan moril, materil, spiritual, hingga selesainya skripsi ini. Kakak saya Sembada Denrineksa Bimorogo dan adik saya Natadadya Puspa Rineksiane yang selalu memberikan semangat dan motivasi untuk menyelesaikan studi. Serta keluarga besar yang selalu mendukung dan memotivasi untuk menyelesaikan studi.
3. Bapak Eddy Prasetyo Nugroho, M.T., selaku pembimbing I yang senantiasa sabar, meluangkan waktu, tenaga dan perhatiannya untuk memberikan bimbingan, pengarahan, motivasi, dan saran-saran berharga bagi penulis dalam penyelesaian skripsi ini.
4. Ibu Dr. Rani Megasari, M.T., selaku pembimbing II yang telah memberikan motivasi, masukan, dukungan kepada penulis untuk menyelesaikan skripsi ini.
5. Ibu Novi Sofia Fitriasari, M.T., selaku DOSen pembimbing akademik yang telah memberikan arahan dan bimbingan selama masa perkuliahan.
6. Seluruh DOSen Departemen Pendidikan Ilmu Komputer yang telah mendidik dan memberikan ilmu hingga penulis dapat menyelesaikan studi.
7. Sahabat-sahabat veteran yaitu Aksan, Faizal, Fajrul, Luthfi, Qays, Reza dan Satria yang senantiasa saling mendukung dan memotivasi agar bisa menyelesaikan studi.

8. Grup Sahabat Edul yaitu Aband, Afil, Alfi, Asep Mulyadi, Asep Rizal, Danang, Dino, Faizal, Giffary, Haris, Faizal, Kuncoro, Rabihi, Handoko, Syandi, Tommy, dan Wiwid yang selalu memberi canda tawa, semangat, motivasi, dan tips dalam proses perkuliahan hingga penyelesaian skripsi ini.
9. Sahabat-sahabat penulis Aam, Luthfi, Gigih dan Reza, terima kasih atas segala semangat, motivasi dan bantuan yang telah diberikan selama proses perkuliahan maupun selama proses pengerjaan skripsi.
10. Teman-teman kelas C2 angkatan 2012, sebagai teman dan sahabat yang selalu ikut mendukung, memotivasi dan mendoakan, terima kasih atas kebersamaan dan kekeluargaannya selama ini.
11. Teman seangkatan Intel 2012 yang juga berjuang bersama demi meraih gelar sarjana dan saling bahu membahu memberikan informasi terkait perkuliahan bahkan lowongan pekerjaan.
12. Serta semua pihak yang tidak dapat disebutkan satu per satu yang turut membantu menyelesaikan skripsi ini.

Penulis menyadari bahwa penyusunan skripsi ini masih belum sempurna. Oleh karena itu, kritik dan saran yang bersifat membangun sangat penulis harapkan guna tercapainya kesempurnaan skripsi ini.

Bandung, Agustus 2019

Penulis,

Samekto Rinekso Pribadi

1202329

IMPLEMENTASI ALGORITMA CM-SPADE DALAM MEMBANGUN MODEL SISTEM DETEKSI *DENIAL OF SERVICE* MENGGUNAKAN SNORT

Oleh

Samekto Rinekso Pribadi – samekto.rinekso@student.upi.edu

1202329

ABSTRAK

Seiring dengan meningkatnya penggunaan komputer, maka aktifitas bisnis dan penyimpanan serta penggunaan data pun sudah mulai dialihkan, dari yang awalnya menggunakan berkas-berkas dokumen, dialihkan menjadi aktifitas komputasi dan data digital yang tersimpan didalam komputer. Meningkatnya kepentingan komputer tentu memunculkan tantangan dan resikonya sendiri. Salah satu risiko dan tantangannya adalah keamanan dari sistem dan jaringan komputer tersebut. Berbagai macam cara sudah dilakukan demi meningkatkan keamanan jaringan komputer, salah satunya adalah menggunakan Intrusion Detection System (IDS). IDS adalah salah salah satu manajemen keamanan yang mampu mendeteksi serangan pada suatu jaringan komputer secara real-time, contohnya serangan *Denial of Service*. Untuk memaksimalkan fungsi deteksi IDS yang mampu mendeteksi serangan yang belum diketahui, maka digunakanlah pendekatan *data mining* dalam membuat IDS yang menerapkan teknik *anomaly based detection*. Pada penelitian ini, teknik *sequential pattern mining* yaitu algoritma CM-SPADE digunakan untuk memunculkan rules IDS yang mampu mendeteksi serangan DOS. Pembuatan model dan rules dilakukan dengan menerapkan algoritma CM-SPADE kepada data KDD Cup tahun 1999. Hasil dari penelitian ini mengungkapkan bahwa penerapan algoritma CM-SPADE mampu menghasilkan rules IDS yang mampu mendeteksi serangan DOS dengan tingkat akurasi sebesar 97,976%.

Kata Kunci**: *Intrusion Detection System, data mining, CM-SPADE, KDD Cup ’99 Dataset, Snort***

IMPLEMENTATION OF CM-SPADE ALGORITHM IN BUILDING DENIAL OF SERVICE DETECTION SYSTEM MODEL USING SNORT

Arranged by

Samekto Rinekso Pribadi – samekto.rinekso@student.upi.edu

1202329

ABSTRACT

Along with the increasing use of computers, business activities and the use of data storage have also begun to changed, from the use of document files which now changed to computing activities and digital data storage stored within the computer. The increasing of computer importance in daily lives also raises it's own challenge and risks. One of the risks and challenge that arose is the security of the computer system and network. Various ways have been done to improve computer network security, one of which is using Intrusion Detection System (IDS). IDS is one of the security management that able to detect attacks on a computer network in real-time, for example Denial of Service (DOS) attacks. To maximize the IDS detection function that is able to detect unknown attacks, a data mining approach is used to create an IDS that uses anomaly based detection techniques. In this study, a sequential pattern mining technique, the CM-SPADE algorithm, is used to generate IDS rules that can detect DOS attacks. Modeling and rules are made by applying the CM-SPADE algorithm to the KDD Cup 1999 data. The results of this study reveal that the application of the CM-SPADE algorithm is able to produce IDS rules that are able to detect DOS attacks with an accuracy rate of 97.976%.

Keyswords: ***Intrusion Detection System, data mining, CM-SPADE, KDD Cup '99 Dataset, Snort***

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

Agrawal, R., & Srikant, R. (1995). Mining sequential patterns. *Proceedings of the Eleventh International Conference on Data Engineering.* Taipei: IEEE.

Bintara, H. (2017, February 16). *Mengenal Snort Sebagai Network Intrusion Detection System (NIDS)*. Diambil kembali dari NETSEC.ID: https://netsec.id/snort-nids/

Darwish, M., Ouda, A., & Capretz, L. F. (2015). A cloud-based secure authentication (CSA) protocol suite for defense against Denial of Service (DOS) attacks. *Journal of Information Security and Applications 20*, 90-98.

Elhag, S., Fernandez, A., Bawakid, A., Alshomrani, S., & Herrera, F. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems. *Expert Systems with Applications*, 193-202.

Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2013). Mining Network Data for Intrusion Detection through Combining SVM with Ant Colony. *Future Generation Computer Systems*.

Fournier-Viger, P., Gomariz, A., Campos, M., & Thomas, R. (2014). Fast Vertical Mining of Sequential Patterns Using Co-occurrence Information. *Advances in Knowledge Discovery and Data Mining*, 40-52.

Garofalakis, M. N., Rastogi, R., & Shim, K. (1999). SPIRIT: Sequential Pattern Mining with Regular Expression Constraints. *25th International Conference on.* Edinburgh: Morgan Kaufmann Publishers.

Gavrilis, D., & Dermatas, E. (2005). Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. *Computer Networks 48*, 235-245.

Gupta, M., & Shrivastava, S. K. (2015). Intrusion Detection System based on SVM and BeeColony. *International Journal of Computer Applications*.

Hoque, M. S., Mukit, M. A., & Bikas, M. A. (2012). An implementation of intusion detection system using genetic algorithm. *International Journal of Network Security & Its Applications*.

Huynh, B., Trinh, C., Huynh, H., Van, T.-T., Vo, B., & Snasel, V. (2018). An efficient approach for mining sequential patterns using multiple threads on very large databases. *Engineering Applications of Artificial Intelligence*, 242-251.

Irvine. (1999, October 28). *KDD Cup 1999 Data*. Diambil kembali dari The UCI KDD Archive: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

KDD CUP ARCHIVES. (2018). Diambil kembali dari KDD: https://www.kdd.org/kdd-cup

Kumar, P. A., & Selvakumar, S. (2013). Detection of distributed denial of service attacks using an ensemble of adaptive and hybird neuro-fuzzy systems. *Computer Communication*, 303-319.

Mason, R. D., & Lind, D. A. (1996). *Teknik Statistik untuk Bisnis & Ekonomi Jilid 1*. Jakarta: Erlangga.

Mohammed, M. N., & Sulaiman, N. (2012). Intrusion Detection System Based on SVM for WLAN. *Procedia Technology 1*, 313-317.

Mooney, C. H., & Roddick, J. F. (2013). Sequential Pattern Mining: Approaches and Algorithms. *ACM Computing Surveys*.

Ramos, V., & Abraham, A. (2005). ANTIDS: Self Organized Ant-Based Clustering Model for Intrusion Detection System. *Soft Computing as Transdisciplinary Science and Technology*, 977-986.

Ravale, U., Marathe, N., & Padiya, P. (2015). Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function. *International Conference on Advanced Computing Technologies and Applications* (hal. 428-435). Procedia Computer Science.

S., S. A., P., A., S., A., & C., V. (2014). An approach for IDS by combining SVM and ant colony algorithm. *International Journal of Research in Engineering and Technology*, 459-465.

Seo, D., Lee, H., & Perrig, A. (2013). APFS: Adaptive Probabilistic Filter Scheduling against distributed denial-of-service attacks. *Computer & Security 39*, 399-385.

Srikant, R., & Agrawal, R. (1996). Mining sequential patterns: Generalizations and performance improvements. *5th International Conference on Extending Database Technology Avignon.* Perancis.

Zaki, M. J. (2001). SPADE: An Efficient Algorithm for Mining Frequent Sequences. *Machine Learning*, 31-60.