SISTEM PENCEGAHAN SERANGAN *BOTNET* DENGAN METODE *SUPPORT VECTOR MACHINE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

AT THORIQ FITRIANSYAH

09011181621025

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA 2021

LEMBAR PENGESAHAN

SISTEM PENCEGAHAN SERANGAN *BOTNET* DENGAN METODE *SUPPORT VECTOR MACHINE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

AT THORIQ FITRIANSYAH

09011181621025

Indralaya, 22 Maret 2021

Mengetahui,

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Deris Stiawan, M.T., Ph.D	Ahmad Heryanto, S.Kom., M.T.
NIP. 197806172006041002	NIP. 197012220150410 02

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis
Tanggal : 11 Februari 2021

Tim Penguji:

1. Ketua : Ahmad Zarkasi, M.T.
2. Sekretaris I : Deris Stiawan, M.T., Ph.D.
3. Sekretaris II : Ahmad Heryanto, S.Kom., M.T.
4. Anggota I : Huda Ubaya, M.T.

Mengtahui,
Ketua Jurusan Sistem Komputer

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : At Thoriq Fitriansyah

NIM : 09011181621025

Judul : Sistem Pencegahan Serangan Botnet dengan Metode Support Vector Machine

Hasil Pengecekan Software Turnitin : 17%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. 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 dalam keadaan sadar dan tidak dipaksakan.

Indralaya, 21 Maret 2021

Yang menyatakan

METERAI TEMPEL

C6F1AAHF596425848

6000

ENAM RIBU RUPIAH

At Thoriq Fitriansyah

NIM. 09011181621025

HALAMAN PERSEMBAHAN

"Sesungguhnya bersama kesulitan itu pasti ada kemudahan. Maka apabila kamu telah selesai(dari sesuatu urusan), kerjakanlah dengansungguh-sungguh (urusan) yanglain, dan hanya kepada Tuhanmulah hendaknya kamu berharap." (QS: 94: 6-8)

"**Experience is the best teacher" (Sidu)**

Skripsi ini saya persembahkan khusus untuk :

- Almarhumah Mama (Neneng Huliah) dan Papa (M. Firdaus) tercinta yang tak pernah berhenti memanjatkan do'a, memotivasi, mendidik dan mengorbankan segala hal kepada putranya demi menggapai cita-cita yang diinginkan
- Seluruh keluarga yang berperan, membantu dan ikut andil dalam perjalananku menuju kesuksesan
- Teman-teman satu grup riset yang selalu menjadi tempat berdiskusi dan bertanya dikala susah, dan
- Dosen pembimbing terbaik yang pernah ada, Bapak Deris Stiawan M.T., Ph.D. dan Bapak Ahmad Heryanto S.Kom., M.T.

Terimakasih banyak…

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur Penulis panjatkan kehadirat Allah SWT, karena berkat rahmat dan karunia-Nya baik berupa pikiran, ilmu pengetahuan mupun kesehatan dan kekuatan sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul ***"Sistem Pencegahan serangan Botnet dengan Metode Support Vector Machine".***

Pada penyusunan tugas akhir ini, tidak terlepas dari bantuan, bimbingan, ajaran serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah dan karunia-Nya kepada penulis dalam penyusunan tugas akhir ini.
2. Orangtua tercinta yang selalu memberikan semangat dan do'a serta keluarga besar penulis yang tersayang.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, M.T., Ph.D selaku pembimbing 1 dan Bapak Ahmad Heryanto S.Kom., M.T. selaku pembimbing 2 Tugas Akhir.
5. Bapak Dr. Ir. Bambang Tutuko M.T., selaku Dosen Pembimbing Akademik.
6. Mbak Reny yang sangat baik, selaku Admin Jurusan Sistem Komputer.
7. Kakak-kakak tingkat yang menjadi panutan, teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2016 terkhusus kelas A, serta semua pihak yang tidak dapat penulis cantumkan satu persatu.
8. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Diriku sendiri yang sangat amat kuat, sabar, dan tabah mengerjakan tugas akhir ini.

Penulis menyadari bahwa masih ada banyak kekurangan dalam laporan tugas akhir ini. Mengingat kurangnya pengetahuan dan pengalaman penulis.

Untuk itu segala kritik dan saran, sangatlah penting bagi penulis.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Wa'alaikumsalam Warahmatullahi Wabarakatuh.

Indralaya, 21 Maret 2021

Penulis

At Thoriq Fitriansyah

BOTNET ATTACK PREVENTION SYSTEM USING SUPPORT VECTOR MACHINE

At Thoriq Fitriansyah (0901118161025)
Departement of Computer System, Faculty of Computer Science,
Sriwijaya University
Email: atthoriq8@gmail.com

ABSTRACT

Intrusion Prevention System is a system that combines firewall techniques and Intrusion Detection System to overcome threats on a network with a network that then provides a warning. In contrast to IDS, IPS provides a response to traffic that is considered an attack and that traffic. The data set used in this research is Stratosphere CTU-25-5 which will compile into the snort IDS engine to get attack patterns from Botnet attacks, once recognized and the proper rules have been supported then the results of the process are validated using Machine Learning with the Support method. Vector Machine and an accuracy value of 98.3%. Furthermore, Suricata Engine is used as an IPS system to be stored, and Botnet attack packages, specifically caused by Zeus Malware. This attack aims to sneak malware to infect computers and reports to become part of the botnet. This system will only order packages based on the rules used (rule-based).

Kata Kunci : Intrusion Prevention System, Botnet, Zeus Malware, CTU 25-5, Suricata

Mengetahui,

Pembimbing I Tugas Akhir

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

Pembimbing II Tugas Akhir

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

Ketua Jurusan Sistem Komputer

Dr. Ir. H Sukemi, M.T.
NIP. 196612032006041

SISTEM PENCEGAHAN SERANGAN BOTNET DENGAN METODE SUPPORT VECTOR MACHINE

At Thoriq Fitriansyah (0901118161025)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email: atthoriq8@gmail.com

ABSTRAK

Intrusion Prevention System merupakan sistem yang menggabungkan teknik firewall dan Intrusion Detection System untuk mendeteksi ancaman pada keamanan jaringan dengan memeriksa lalu lintas jaringan memberikan alert. Berbeda dengan IDS, IPS memberikan respon terhadap traffic yang di anggap serangan dan memblokir traffic tersebut. Dataset yang digunakan dalam penelitian ini adalah Stratosphere CTU-25-5 yang akan di compile kedalam snort IDS engine untuk mendapatkan pola serangan dari serangan Botnet, setelah dikenali serta rules yang tepat sudah di dapatkan kemudian hasil dari proses tersebut divalidasi menggunakan Machine Learning dengan metode Support Vector Machine dan di peroleh nilai akurasi sebesar 98,3%. Selanjutnya digunakan Suricata Engine sebagai sistem IPS yang akan mengenali, dan memblokir paket serangan Botnet, spesifiknya disebabkan oleh Malware Zeus. Serangan jenis ini bertujuan untuk menyusupkan malware untuk menginfeksi komputer dan membuatnya menjadi bagian dari botnet. Sistem ini hanya akan memblokir paket hanya berdasarkan rules yang digunakan (rule based).

Kata Kunci : Intrusion Prevention System, Botnet, Malware Zeus, CTU 25-5, Suricata

Mengetahui,

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

Ketua Jurusan Sistem Komputer

Dr. Ir. H Sukemi, M.T.
NIP. 196612032006041

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I. PENDAHULUAN

1.1 LATAR BELAKANG

1

Sejak tahun 2003 *botnet* menjadi salah satu ancaman paling agresif di dalam jaringan komputer, bahkan serangan botnet terus meningkat hingga 58% di wilayah asia pasifik [1, 2] bahkan pada bulan juli 2020 Trend Micro researchers menemukan jenis *botnet* baru yang dapat memindai perangkat-perangkat yang terekspos. Menurut [3] laporan CVE-2020-10173 *botnet* ini dapat mengeksploitasi *router*, DVRs, IP kamera, dan beberapa perangkat dari vendor popular.

Network Intrusion Detection System (NIDS) [4] merupakan salah satu solusi untuk mengatasi ancaman keamanan pada jaringan komputer. IDS merupakan perangkat lunak yang yang dapat mendeteksi anomaly pada traffic. Sedangkan *Intrusion Prevention System* (IPS) adalah sistem yang menggabungkan teknik firewall dengan IDS untuk mendeteksi dan memblokir malicious traffic [5].

Penelitian sebelumnya [6] membahas cara mendeteksi *botnet* menggunakan beberapa metode machine learning antara lain *Naïve Bayes, Naïve Bayes Tree, K-Nearst Neighor* dan *Random Forest*. Sedangkan pada penelitian lain [7] menggunakan algoritma *Support Vector Machine* untuk mendeteksi dan di dapatkan akurasi yang baik. SVM [8] adalah metode data mining berbasis kernel yang banyak digunakan untuk klasifikasi biner dan terbukti memiliki tingkat akurasi yang tinggi untuk mengklasifikasi pola paket di jaringan komputer.

Dalam kasus ini peneliti akan memvalidasi dan mengimplementasikan metode *machine learning* yaitu Support *Vector Machine* pada server IPS dengan performa *suricata engine* untuk mendeteksi dan melakukan drop pada *traffic*

jaringan yang di sinyalir sebagai botnet. Penerapan metode SVM ini untuk mengklasifikasi apakah benar traffic tersebut merupakan serangan *botnet* atau traffic normal. Sistem IPS ini kedepannya di harapkan dapat menjadi sistem yang lebih selektif dan responsif dalam mendeteksi traffic serangan.

1.2. TUJUAN

Dalam penelitian ini terdapat beberapa tujuan yang akan dicapai yaitu sebagai berikut:

1. Mendeteksi traffic serangan *Botnet* yang disebabkan oleh *malware zeus*
2. Mengimplementasikan metode *Machine Learning* dengan *Algoritma SVM* untuk mendeteksi salah satu jenis serangan *Botnet.*
3. Merancang sistem IPS untuk mencegah serangan *Botnet*.
4. Memblokir akses serangan *botnet* yang disebabkan oleh *malware zeus* pada saat dilakukan simulasi.
5. Menganalisa dan menghitung akurasi yang didapatkan dari metode yang digunakan dalam penelitian.

1.3 MANFAAT

Terdapat beberapa manfaat yang di harapkan dalam penelitian ini yaitu:

1. Kedepannya akan memberikan kemudahan dalam mengenali pattern atau pola dari serangan *botnet*.
2. Dapat mengklasifikasikan *anomaly traffic* yang disebabkan oleh aktifitas *malware zeus.*
3. Dapat memberikan informasi mengenai performa metode *SVM* dalam mengklasifikasi serangan *botnet*.
4. Mencegah serangan *botnet* yang disebabkan oleh *malware zeus.*

1.4. RUMUSAN MASALAH

Berdasarkan latar belakang masalah yang ada, permasalahan yang akan di bahas pada penelitian ini ada dua yaitu:

1. Melakukan paket *sniffing* dan mengolah data yang akan digunakan sebagai data training untuk metode model SVM
2. Bagaimana algoritma *Support Vector Machine* (SVM) ini dapat mengklasifikasi paket serangan *Botnet* atau paket data normal.
3. Mendeteksi dan memblokir akses traffic *Botnet*.

1.5. BATASAN MASALAH

Batasan masalah pada penelitian ini yaitu mengenali pola serangan *botnet* yang disebabkan oleh *malware zeus dalam penelitian ini h*anya membahas cara mencegah salah satu variasi dari serangan *botnet* yang disebabkan oleh malware zeus. Metode yang digunakan untuk memvalidasi hasil *performa suricata engine* adalah *Support Vector Machine*.

1.6. METODOLOGI PENELITIAN

Berikut merupakan langkah-langkah atau metode yang akan digunakan dalam penelitian ini yaitu :

1. Studi Literatur

Pada Tahap ini dilakukan pencarian masalah yang sesuai dengan tujuan untuk diangkat sebagai penelitian. Selanjutnya mencari sumber-sumber seperti paper, jurnal, conference dan lainnya tentu saja yang berhubungan dengan penelitian ini.

2. Tahap Perancangan Sistem

Tahap kedua ini akan membahas masalah proses bagaimana sistem

tersebut di rancang dan di bangun untuk mengklasifikasi untuk melakukan deteksi dan mencegah serangan botnet menggunakan algoritma support vector machine. Tahap ini dibagi menjadi dua skenario yaitu *intrusion detection system* (IDS) dan *intrusion prevention system* (IPS)

3. Tahap Pengujian

Pada tahap ini dilakukan pengujian berdasarkan metode yang digunakan dalam penelitian dan metode-metode yang digunakan oleh penelitian sebelumnya, sehingga didapatan hasil yang sesuai.

4. Analisa

Tahap ini dilakukan pengolahan data dan analisa data yang didapatkan dari hasil pengujian yang dilakukan sebelumnya untuk mendapatkan data yang aktual. Kemudian hasil akan dianalisis dengan tujuan untuk mengetahui kekurangan pada hasil perancangan sistem tersebut.

5. Kesimpulan

Tahapan ini merupakan langkah akhir, hasil dari semua langkah yang dilakukan sebelumnya akan dirumuskan menjadi suatu kesimpulan.

1.7 SISTEMATIKA PENULISAN

Agar dapat mempermudah proses penyusunan dan memperjelas isi dari setiap bab maka akan dibuat sistematika dalam penulisan yaitu sebagai berikut :

BAB I. PENDAHULIAN

BAB I berisi penjelasan secara singkat dan sistematis mengenai topik-topik dalam penelitian yang meliputi latar belakang, tujuan, manfaat, rumusan masalah, dan batasan masalah dan terakhir sistematika penulisan metodologi.

BAB II. TINJAUAN PUSTAKA

BAB II berisi landasan teori dari *Intrusion Prevention System, Botnet,* apa itu *Machine Learning,* dan *Support Vector Machine* yang tentu berhubungan dengan penelitian.

BAB III. METODOLOGI PENELITIAN

BAB III menjelaskan secara ilustratif, bagaimana langkah-langkah yang dilakukan pada penelitian. Penjelasannya meliputi tahapan perancangan sistem dan penerapan metode dalam penelitian ini.

BAB IV. HASIL DAN ANALISA

BAB IV menjelaskan hasil yang didapatkan dari pengujian serta dilakukan analisis terhadap data yang diperoleh pengujian.

BAB V. KESIMPULAN

BAB V berisi beberapa kesimpulan yang didapatkan dari hasil penelitian, serta menjawab tujuan yang ditargetkan akan tercapai pada BAB I.

DAFTAR PUSTAKA

[1] N. Y. Lee and H. J. Chiang, "The research of botnet detection and prevention," *ICS 2010 - Int. Comput. Symp.*, pp. 119–124, 2010, doi: 10.1109/COMPSYM.2010.5685534.

[2] F. Haddaddi and A. N. Zincir-heywood, "Botnet Behaviour Analysis: How would a data analytics-based system with minimum a priori information perform?," pp. 1–20, 2016, doi: 10.1002/nem.1977.

[3] "Mirai Botnet Downloader Module Scans For Most Recent Critical Vulnerabilities." [Online]. Available: https://cyware.com/news/mirai- botnet-downloader-module-scans-for-most-recent-critical- vulnerabilities-2060213f. [Accessed: 12-Dec-2020].

[4] 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.*, vol. 4, pp. 217–221, 2010, doi: 10.1109/ICETC.2010.5529697.

[5] D. Stiawan, A. Y. I. Shakhatreh, M. Y. Idris, A. B. Kamarulnizam, and H. A. Abdul, "Intrusion prevention system: A survey," *J. Theor. Appl. Inf. Technol.*, vol. 40, no. 1, pp. 44–54, 2012.

[6] A. A. Awad and S. A. Salem, "A Network-based Framework for RAT- Bots Detection," pp. 128–133, 2017.

[7] A. A. Awad, S. G. Sayed, and S. A. Salem, "Collaborative Framework for Early Detection of RAT-Bots Attacks," *IEEE Access*, vol. 7, pp. 71780–71790, 2019, doi: 10.1109/ACCESS.2019.2919680.

[8] M. Kruczkowski and E. Niewiadomska-Szynkiewicz, "Support vector machine for malware analysis and classification," *Proc. - 2014*

IEEE/WIC/ACM Int. Jt. Conf. Web Intell. Intell. Agent Technol. - Work. WI-IAT 2014, vol. 2, pp. 280–283, 2014, doi: 10.1109/WI- IAT.2014.127.

[9] M. F. I. SAPUTRA, "Deteksi Serangan Remote to Local (R2L) Menggunakan Metode Support Vector Machine (SVM)m," 2019.

[10] S. Ryu and B. Yang, "A Comparative Study of Machine Learning Algorithms and Their Ensembles for Botnet Detection," *J. Comput. Commun.*, vol. 06, no. 05, pp. 119–129, 2018, doi: 10.4236/jcc.2018.65010.

[11] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," *Int. Conf. Inf. Netw.*, pp. 712–717, 2017, doi: 10.1109/ICOIN.2017.7899588.

[12] R. Baeyens, R. Berkvens, W. Daems, J.-P. Baeyens, M. Goossens, and M. Weyn, "Host Based Intrusion Detection and Prevention Model Against DDoS Attack in Cloud Computing," *Adv. P2P, Parallel, Grid, Cloud Internet Comput.*, vol. 13, pp. 722–732, 2018, doi: 10.1007/978- 3-319-69835-9.

[13] J. Singh and M. J. Nene, "A Survey on Machine Learning Techniques for Intrusion Detection Systems," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 11, pp. 4349–4355, 2013.

[14] A. Sawant, "A Comparative Study of Different Intrusion Prevention Systems," *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, pp. 1–5, 2018, doi:10.1109/ICCUBEA.2018.8697500.

[15] D. Mudzingwa and R. Agrawal, "A study of methodologies used in intrusion detection and prevention systems (IDPS)," *Conf. Proc. - IEEE SOUTHEASTCON*, no. September, 2012, doi: 10.1109/SECon.2012.6197080.

[16] K. Dist and K. Dist, "Intrusion Detection System Methodologies Based

on Data Analysis," vol. 5, no. 2, pp. 10–20, 2010.

[17] A. Jamdagni, "Payload-based Anomaly Detection in HTTP Traffic," no. November, p. 190, 2012.

[18] S. Ali, R. Shah, and B. Issac, "Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System," 2017.

[19] H. Xia, "Research on Bot-Net Prevention and Control Technology Based on P2P," *Proc. 2018 2nd IEEE Adv. Inf. Manag. Commun. Electron. Autom. Control Conf. IMCEC 2018*, no. Imcec, pp. 1986–1990, 2018, doi: 10.1109/IMCEC.2018.8469569.

[20] G. Vormayr, T. Zseby, and J. Fabini, "Botnet Communication Patterns," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2768–2796, 2017, doi: 10.1109/COMST.2017.2749442.

[21] S. Saiyod and Y. Chanthakoummane, "Improving Intrusion Detection on Snort Rules for Botnet Detection," pp. 191–212, 2016, doi: 10.13052/jsn2445-9739.2016.011.

[22] R. Layton and A. Azab, "Authorship analysis of the zeus botnet source code," *Proc. - 5th Cybercrime Trust. Comput. Conf. CTC 2014*, pp. 38– 43, 2015, doi: 10.1109/CTC.2014.14.

[23] T. I. U. of B. Saad Hafeez B.Eng. and A, "Deep Packet Inspection using Snort," *Deep Pack. Insp. using Snort*, p. 24, 2017.

[24] Z. Zhou, Z. Chen, T. Zhou, and X. Guan, "The study on network intrusion detection system of snort," *2010 Int. Conf. Netw. Digit. Soc. ICNDS 2010*, vol. 2, pp. 194–196, 2010, doi: 10.1109/ICNDS.2010.5479341.

[25] H. S. Guo, W. J. Wang, and C. Q. Men, "A novel learning model-kernel granular support vector machine," *Proc. 2009 Int. Conf. Mach. Learn. Cybern.*, vol. 2, no. July, pp. 930–935, 2009, doi: 10.1109/ICMLC.2009.5212413.

[26] H. Zhang, C. He, M. Yu, and J. Fu, "Texture feature extraction and classification of SEM images of wheat straw/polypropylene composites in accelerated aging test," *Adv. Mater. Sci. Eng.*, vol. 2015, no. September 2015, 2015, doi: 10.1155/2015/397845.

[27] A. Vault, "A Search Engine for Threats." [Online]. Available: https://www.threatcrowd.org/sitemaps/domains2226.htm. [Accessed: 28-Jan-2021].

[28] Jaime Blasco, "[Emerging-Sigs] Malware Connectivity Check," 2017. [Online].Available: http://lists.emergingthreats.net/pipermail/emerging-sigs/2014-November/025159.html. [Accessed: 28-Jan-2021].

[29] Anonymous, "Packet Total d7c37c694532a1fe74c94d5c5430b4f4 HTTPAnalysis," 2017. [Online]. Available: https://packettotal.com/app/analysis?id=d7c37c694532a1fe74c94d5c5430b4f4&name=http. [Accessed: 28-Jan-2021].