VISUALISASI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *K-MEANS*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

HAFIZD SETIAWAN

09011182025004

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

VISUALISASI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *K-MEANS*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :
Hafizd Setiawan
09011182025004

Indralaya, 4/6/ Mei 2024

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M.T.	**Prof. Deris Stiawan, M.T.**
NIP. 196612032006041001	**NIP. 197806172006041002**

AUTHENTICATION PAGE

VISUALIZATION OF METASPLOIT TROJAN ATTACKS ON ANDROID USING K-MEANS METHOD

SKRIPSI

Submitted To Complete One Of The Requirements For Obtaining A Bachelor's Degree in Computer Science

By :

HAFIZD SETIAWAN

09011182025004

Palembang, 9 Mei 2024

Acknowledge,

Head Of Computer System Departement	Final Project Advisor
Dr. Ir. Sukemi, M.T.	**Prof. Deris Stiawan, M.T.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Rabu**

Tanggal : **22 Mei 2024**

Tim Penguji :

1. **Ketua** : **Ahmad Heryanto, M.T.**
2. **Sekretaris** : **Abdurahman, S.Kom.,M.Han**
3. **Penguji** : **Dr. Ahmad Zarkasi, M.T.**
4. **Pembimbing** : **Prof. Deris Stiawan, M.T., PH.D.**

Mengetahui, 4/6/24
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang Bertanda Tangan Di Bawah Ini :

Nama	:	Hafizd Setiawan
NIM	:	09011182025004
Judul	:	VISUALISASI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *K-MEANS.*

Hasil Pengecekkam Software iThenticate/Turnitin : 8%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

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

Indralaya, 27 Mei 2024
Penulis,

Hafizd Setiawan
NIM.09011182025004

KATA PENGANTAR

Puji syukur penulis pajatkan kepada Tuhan Yang Maha Esa, karena dengan rahmat dan karunia-Nya penulis dapat menyelesaiakan Tugas Akhir ini yang berjudul ***"VISUALISASI SERANGAN TROJAN METASPLOIT PADA ANDROID DENGAN METODE K-MEANS".***

Dalam laporan ini Penulis bertujuan untuk memberikan pemahaman yang lebih dalam tentang serangan payload pada perangkat Android dengan fokus pada visualisasi data yang dihasilkan dari serangan tersebut. Dengan menggunakan algoritma K-Means, penelitian ini berusaha untuk mengelompokkan data yang terkumpul dari serangan dari android ke dalam berbagai kelompok yang memungkinkan identifikasi pola-pola yang mungkin terjadi.

Pada kesempatan ini, saya sebagai penulis mengucapkan terima kasih kepada pihak yang telah membantu dalam penyusunan Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur dan terima kasih sebesar – besarnya kepada :

1. Allah SWT, atas berkat, rahmat dan karunia-Nya yang telah diberikan kepada penulis, sehingga penulis dapat menyelesaikan Tugas Akhir ini dalam keadaan yang berjalan baik dan lancar.
2. Kedua orang tua saya yang telah memberikan doa, dukungan dan juga semangat kepada penulis selama ini.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom, M.T. selaku Dosen Akademik yang telah memberikan banyak ilmu.
6. Bapak Prof. Deris Stiawan, M.T. selaku Dosen Pembimbing Tugas Akhir yang telah memberikan banyak ilmu dan membimbing dalam pengerjaan Tugas Akhir ini.
7. Orang-orang tersayang, saudara tak sedarah, serta sahabat di luar lingkungan

kampus yang selalu memberikan semangat, dukungan dan motivasi dalam menyelesaikan laporan ini.

8. Dan semua pihak yang telah membantu penulis.

Penulis menyadari bahwa masih banyak kekurangan di dalam Tugas Akhir ini, sehingga masih jauh dari kata sempurna. Untuk itu kiranya berkenan kritik serta saran yang membangun sangat diperlukan dalam rangka penyegeraan perbaikan Tugas Akhir ini sebagai ide baru untuk pembahasan penelitian yang berkaitan.

Indralaya, Juni 2024

Penulis,

Hafizd Setiawan

09011182025004

VISUALISASI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *K-MEANS*

HAFIZD SETIAWAN
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : hafizdsetiawan21@gmail.com

ABSTRAK

K-Means clustering adalah alat yang digunakan untuk menentukan struktur cluster dari kumpulan data yang telah diidentifikasi oleh kemiripannya yang kuat dengan cluster lain atau perbedaannya yang kuat dari cluster lain. Dalam makalah lain, dikatakan bahwa metode kerja algoritma *K-Means* memerlukan penggunaan centroid sebagai prototipe cluster dan hasil cluster sebelumnya sebagai outputnya. Dataset berasal dari percobaan hasil riset COMNETS. K-Means berhasil mengelompokkan 2 cluster dengan *silhouette score* sebesar 0,81 dan hasil *elbow method* terdapat penurunan yang signifikan pada 2 cluster. Hasil visualisasi paralel coordinat menunjukan adanya pola serangan dari trojan metasploit. Validasi menggunakan *Confusion Matrix* menunjukan bahwa model memperoleh akurasi sebesar 85.94%.

kata kunci : *K-means Clustering, Cyber Attack, Metasploit, Silhouette Score.*

VISUALIZATION OF METASPLOIT TROJAN ATTACKS ON ANDROID USING K-MEANS METHOD

HAFIZD SETIAWAN
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : hafizdsetiawan21@gmail.com

ABSTRACT

K-Means clustering is a tool used to determine the cluster structure of a dataset identified by its strong similarity to other clusters or its strong difference from other clusters. In another paper, it is stated that the working method of the K-Means algorithm requires the use of centroids as cluster prototypes and previous cluster results as its output. The dataset originates from the COMNETS research experiment. K-Means successfully clustered into 2 clusters with a silhouette score of 0.81, and the elbow method results indicated a significant drop at 2 clusters. The parallel coordinates visualization showed patterns of attacks from the Metasploit trojan. Validation using the Confusion Matrix showed that the model achieved an accuracy of 85.94%.

Keyword : *K-means Clustering, Cyber Attack, Metasploit, Silhouette Score.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perangkat Android telah menjadi bagian integral dari kehidupan sehari-hari, dengan jutaan pengguna yang bergantung pada mereka untuk berbagai aktivitas, termasuk komunikasi, pembayaran, dan penyimpanan informasi pribadi[1]. Dalam era digital yang semakin maju, penggunaan perangkat Android telah menjadi hal yang sangat umum. Perangkat Android digunakan dalam berbagai konteks, mulai dari perangkat pribadi hingga perangkat bisnis, dan menyimpan berbagai jenis data pribadi dan sensitif.[2].Kemudahan aksesibilitas dan fleksibilitas dalam penggunaan aplikasi juga salah satu alasan utama di balik popularitasnya. Namun, popularitas yang tinggi ini juga menjadikan perangkat Android sebagai target yang menarik bagi penyerang siber,salah satunya yaitu dengan mengirimkan *Trojan Metasploit* ke perangkat Andorid korban [3].

Metasploit adalah sebuah platform perangkat lunak yang digunakan untuk pengujian penetrasi dan pengembangan keamanan. Ini mencakup seperangkat alat dan sumber daya yang dirancang untuk membantu para profesional keamanan dan peneliti keamanan dalam mengidentifikasi dan memanfaatkan kelemahan keamanan pada sistem komputer[4].*Trojan Metasploit* seringkali menjadi pilihan utama bagi penyerang siber yang ingin mengambil alih atau meretas perangkat Android. Dalam strategi ini, penyerang menggunakan *Metasploit* untuk menyisipkan kode berbahaya ke dalam perangkat, memungkinkan mereka untuk mencuri data pribadi, merusak perangkat, atau melancarkan serangan jahat lainnya. Serangan menggunakan *Trojan Metasploit* dapat memiliki dampak serius, baik pada tingkat individu maupun pada tingkat perusahaan atau organisasi[5].

Pada penelitian ini, penulis berfokus pada implementasi serangan *Trojan Metasploit* dengan penekanan pada sistem keamanan. Melalui penerapan teknik penetrasi dan eksploitasi yang dimiliki oleh *Metasploit.* Serangan ini akan difokuskan pada keberhasilan meretas perangkat Android sebagai studi kasus utama. Penggunaan *Metasploit* akan diarahkan untuk menyusup ke dalam perangkat Android dan menyisipkan kode berbahaya, memberikan penyerang

kontrol penuh terhadap perangkat tersebut. Penetrasi dalam konteks ini dapat mencakup ekstraksi data pribadi, merusak fungsi perangkat, atau bahkan menjalankan tindakan jahat lainnya.

Penggunaan Algoritma *K-Means* dalam visualisasi serangan trojan *Metasploit* didasarkan pada kemampuannya untuk secara otomatis mengelompokkan data serangan trojan ke dalam kelompok dengan pola serupa. Algoritma ini memudahkan identifikasi dan pemahaman terhadap karakteristik serangan, termasuk pola-pola tersembunyi yang mungkin sulit ditemukan melalui analisis manual. Keunggulan lainnya adalah skalabilitas algoritma, yang memungkinkan penanganan efisien terhadap volume data serangan yang besar[6]. Selain itu, *K-Means* merupakan metode yang sederhana dan efisien[7], memungkinkan analisis yang cepat dan hasil visualisasi yang jelas.

Berdasarkan latar belakang yang telah di uraikan diatas, maka penulis memutuskan untuk mengambil judul pada Tugas Akhir ini yaitu "Visualisasi Serangan *Trojan Metasploit* Pada Android Dengan Metode *K-Means*"**.**

1.2 Perumusan Masalah

Adapun perumusan masalah dalam laporan tugas akhir ini, yaitu :

1. Bagaimana melakukan visualisasi serangan *Trojan Metasploit* menggunakan metode *K-Means*?.
2. Bagaimana distribusi cluster dan menggunakan algoritma K-means untuk menentukan cluster terbaik?.
3. Bagaimana kinerja dari metode *K-Means* dalam mengidentifikasi dan memvisualisasikan serangan Trojan Metasploit?.

1.3 Tujuan Penelitian

Adapun tujuan penulisan tugas akhir ini yaitu sebagai berikut :

1. Melakukan visualisasi serangan *Trojan Metasploit.*
2. Melakukan distribusi cluster dan memahami cluster terbaik pada dataset.
3. Membuat grafik pola serangan *Trojan Metasploit* dan memvisualisasikannya.

1.4 Manfaat Penelitian

Manfaat dari penulisan tugas akhir ini yaitu sebagai berikut :

1. Penggunaan metode Silhouette dan Elbow dalam pengujian cluster dimanfaatkan untuk memperoleh pemahaman tentang kualitas serta model cluster yang optimal.
2. Dapat memvisualisasikan dan mengolah data terhadap serangan *Trojan Metasploit*.
3. Dapat mempelajari bagaimana pola serangan *Trojan Metasploit*

1.5 Batasan Masalah

Batasan masalah dalam penulisan tugas akhir ini yaitu :

1. Dataset yang digunakan adalah dataset yang dibuat dari hasil riset Lab COMNETS(*Communication Network and Information Security Research Group*)
2. Penelitian ini hanya menggunakan metode algoritma *K-Means Clustering.*
3. Penelitian ini hanya memvisualisasikan serangan *Trojan Metasploit*, tidak membahas bagaimana cara mencegahnya.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Metode Studi Pustaka dan Literatur

   Metode ini digunakan untuk mencari referensi,termasuk buku dan jurnal yang diperlukan dan relevan dengan penelitian ini.
2. Metode Konsultasi

   Pada metode ini dengan berbagai pihak lain diantaranya dosen dan praktisi.
3. Pemrosesan Data

   Pada tahap ini membahas bagaiamana pengolahan data dan bagaimana data diproses.
4. Visualisasi

   Tahapan dilakukan dengan memasukan data dalam bentuk grafik dengan menggunakan parallel koordinat serta mencari klaster terbaik.
5. Analisa dan Kesimpulan

   Pada langkah ini,Hasil tersebut dianalisa dan kemudian ditarik kesimpulan

tentang masalah dan hasil tersebut.

1.7 Sistematika Penulisan

Sistematika Penulisan yang dilakukan dalam Tugas Akhir ini adalah :

BAB I PENDAHULUAN

Bab pertama membahas latar belakang, tujuan, manfaat, Batasan, Metodologi Penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas studi literatur dan memberikan penjelasan jurnal yang terkait pada penelitian ini sebagai referensi penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini membahas bagaimana langkah-langkah yang diambil peneliti selama penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil dan pembahasan penelitian penulis dibahas dalam bab ini.

BAB V KESIMPULAN DAN SARAN

Bab ini mencakup kesimpulan yang diambil oleh peneliti sebagai tanggapan atas tujuan penelitian ini, dan rekomendasi untuk hasil yang diperoleh pada tugas akhir

DAFTAR PUSTAKA

[1] Y. Li, J. Jang, X. Hu, and X. Ou, "Android Malware Clustering Through Malicious Payload Mining," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10453 LNCS, pp. 192–214, 2017, doi: 10.1007/978-3-319-66332-6_9.

[2] A. Feizollah, N. B. Anuar, R. Salleh, and F. Amalina, "Comparative study of k-means and mini batch k-means clustering algorithms in android malware detection using network traffic analysis," *Proc. - 2014 Int. Symp. Biometrics Secur. Technol. ISBAST 2014*, no. February, pp. 193–197, 2015, doi: 10.1109/ISBAST.2014.7013120.

[3] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A Review of Android Malware Detection Approaches Based on Machine Learning," *IEEE Access*, vol. 8, pp. 124579–124607, 2020, doi: 10.1109/ACCESS.2020.3006143.

[4] R. Seema and N. Ritu, "Penetration Testing Using Metasploit Framework : an Ethical Approach," *Int. Res. J. Eng. Technol.*, vol. 06, no. 08, pp. 538–542,2019,[Online].Available:https://www.academia.edu/40379823/IRJET_PENETRATION_TESTING_USING_METASPLOIT_FRAMEWORK_AN_ETHICAL_APPROACH

[5] P. Sharma, C. Lepcha, S. T. Bhutia, and A. Sharma, "Case Study Exploit of Android Devices Using Payload Injected Apk," no. 06, pp. 1552–1557, 2023, [Online]. Available: https://www.irjmets.com/uploadedfiles/paper/issue_6_june_2023/41927/final/fin_irjmets1686539223.pdf

[6] K. P. Sinaga and M. S. Yang, "Unsupervised K-means clustering algorithm," *IEEE Access*, vol. 8, pp. 80716–80727, 2020, doi: 10.1109/ACCESS.2020.2988796.

[7] Y. Zhao and X. Zhou, "K-means Clustering Algorithm and Its Improvement Research," *J. Phys. Conf. Ser.*, vol. 1873, no. 1, 2021, doi: 10.1088/1742-

6596/1873/1/012074.

[8] H. Rathore, S. K. Sahay, P. Chaturvedi, and M. Sewak, “Android Malicious Application Classification Using Clustering,” *Adv. Intell. Syst. Comput.*, vol. 941, pp. 659–667, 2020, doi: 10.1007/978-3-030-16660-1_64.

[9] Z. Wang, Y. Zhou, and G. Li, “Anomaly Detection by Using Streaming K-Means and Batch K-Means,” *2020 5th IEEE Int. Conf. Big Data Anal. ICBDA 2020*, pp. 11–17, 2020, doi: 10.1109/ICBDA49040.2020.9101212.

[10] M. Blumenschein, X. Zhang, D. Pomerenke, D. A. Keim, and J. Fuchs, “Evaluating Reordering Strategies for Cluster Identification in Parallel Coordinates,” *Comput. Graph. Forum*, vol. 39, no. 3, pp. 537–549, 2020, doi: 10.1111/cgf.14000.

[11] Kanika, K. Rani, Sangeeta, and Preeti, “Visual Analytics for Comparing the Impact of Outliers in k-Means and k-Medoids Algorithm,” *Proc. - 2019 Amity Int. Conf. Artif. Intell. AICAI 2019*, pp. 93–97, 2019, doi: 10.1109/AICAI.2019.8701355.

[12] J. Senanayake, H. Kalutarage, and M. O. Al-Kadri, “Android mobile malware detection using machine learning: A systematic review,” *Electron.*, vol. 10, no. 13, pp. 1–34, 2021, doi: 10.3390/electronics10131606.

[13] R. Surendran, T. Thomas, and S. Emmanuel, “A TAN based hybrid model for android malware detection,” *J. Inf. Secur. Appl.*, vol. 54, p. 102483, 2020, doi: 10.1016/j.jisa.2020.102483.

[14] V. Sihag, M. Vardhan, and P. Singh, “A survey of android application and malware hardening,” *Comput. Sci. Rev.*, vol. 39, no. May, 2021, doi: 10.1016/j.cosrev.2021.100365.

[15] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, “Malware Detection Issues, Challenges, and Future Directions: A Survey,” *Appl. Sci.*, vol. 12, no. 17, 2022, doi: 10.3390/app12178482.

[16] B. Wang *et al.*, “Neural cleanse: Identifying and mitigating backdoor attacks in neural networks,” *Proc. - IEEE Symp. Secur. Priv.*, vol. 2019-May, pp.

707–723, 2019, doi: 10.1109/SP.2019.00031.

[17] Y. Gao *et al.*, “Backdoor Attacks and Countermeasures on Deep Learning: A Comprehensive Review,” pp. 1–30, 2020, [Online]. Available: http://arxiv.org/abs/2007.10760

[18] N. I. Aminuddin and Z. Abdullah, “Android Trojan Detection Based on Dynamic Analysis,” *Adv. Comput. Intell. Syst.*, vol. 1, no. 1, pp. 1–7, 2019, [Online]. Available: https://www.fazpublishing.com/acis/index.php/acis/article/view/4

[19] S. Raj and N. K. Walia, “A Study on Metasploit Framework: A Pen-Testing Tool,” *2020 Int. Conf. Comput. Perform. Eval. ComPE 2020*, no. July 2020, pp. 296–302, 2020, doi: 10.1109/ComPE49325.2020.9200028.

[20] H. Iqbal and S. Naaz, “Wireshark as a Tool for Detection of Various LAN Attacks,” *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 833–837, 2019, doi: 10.26438/ijcse/v7i5.833837.

[21] F. J. Ariza-López, J. Rodríguez-Avi, and M. V. Alba-Fernández, “Complete control of an observed confusion matrix,” *Int. Geosci. Remote Sens. Symp.*, vol. 2018-July, pp. 1222–1225, 2018, doi: 10.1109/IGARSS.2018.8517540.

[22] K. G. Liakos, G. K. Georgakilas, S. Moustakidis, P. Karlsson, and F. C. Plessas, “Machine Learning for Hardware Trojan Detection: A Review,” *5th Panhellenic Conf. Electron. Telecommun. PACET 2019*, no. January, pp. 1–6, 2019, doi: 10.1109/PACET48583.2019.8956251.

[23] V. Joseph Raymond and R. Jeberson Retna Raj, “Investigation of Android Malware with Machine Learning Classifiers using Enhanced PCA Algorithm,” *Comput. Syst. Sci. Eng.*, vol. 44, no. 3, pp. 2147–2163, 2023, doi: 10.32604/csse.2023.028227.

[24] K. R. Mim, M. S. Hossain, S. A. Tisha, K. R. Kalpo, M. H. Bakul, and M. S. Hossain, “Traffic Analysis-Based Android SMS Malware Detection Using Machine Learning,” *Lect. Notes Networks Syst.*, vol. 437, no. October, pp. 305–317, 2022, doi: 10.1007/978-981-19-2445-3_20.

[25] K. R. Shahapure and C. Nicholas, “Cluster Quality Analysis Using

Silhouette Score," pp. 2020–2021, 2020, doi: 10.1109/DSAA49011.2020.00096.