Analisis Malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara *Sandbox Custom, Cuckoo Sandbox, dan Falcon Sandbox*

SKRIPSI

HARY ALFAJRI

2107421013

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

TAHUN 2025

Analisis Malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara *Sandbox Custom, Cuckoo Sandbox, dan Falcon Sandbox*

SKRIPSI

Dibuat untuk melengkapi syarat-syarat yang diperlukan
untuk memperoleh diploma empat politeknik

HARY ALFAJRI

2107421013

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
TAHUN 2025

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama :	Hary Alfajri
NIM :	2107421013
Jurusan/Program Studi :	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi :	Analisis Malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara Sandbox Custom, *Cuckoo Sandbox* , dan *Falcon andbox*.

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 24 Juni 2025

Yang Membuat Pernyataan

Hary Alfajri

NIM. 210742101

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama :	Hary Alfajri
NIM :	2107421013
Jurusan/Program Studi :	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi :	Analisis Malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara Sandbox Custom, *Cuckoo Sandbox* , dan *Falcon Sandbox*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu Tanggal **2** Bulan **Juli Tahun 2025**, dan dinyatakan **LULUS**.

Disahkan Oleh

Pembimbing I	Iik Muhamad Malik Matin, S.Kom., M.T.	( )
Penguji I	Defiana Arnaldy, S.Tp., M.Si	( )
Penguji II	Asep Kurniawan, S.Pd., M.Kom.	( )
Penguji III	Fachroni **Arbi Murad, S.Kom., M.Kom.**	( )

Mengetahui:
Jurusan Teknik Informatika dan Komputer Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan penyusunan skripsi ini dengan judul *"Analisis Malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara Sandbox Custom, Cuckoo Sandbox , dan Falcon Sandbox"* ini dengan baik. Penyusunan skripsi ini tidak lepas dari dukungan dan bantuan berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Jurusan Teknik Informatika dan Komputer, yang telah memberikan fasilitas, ilmu pengetahuan, dan lingkungan belajar yang kondusif selama masa studi.
2. Bapak Iik Muhamad Malik Matin, S.Kom., M.T. selaku dosen pembimbing yang telah memberikan arahan dan masukan yang sangat berharga selama proses penyusunan..
3. Kedua orang tua tercinta, kakak dan adik yang senantiasa memberikan doa, dukungan moral, dan motivasi yang tak ternilai harganya.
4. Teman seperjuangan sekaligus rekan satu dosen pembimbing, Layla Rosyidah, terima kasih atas semangat, bantuan, dan kebersamaan selama proses penyusunan skripsi ini. Dukunganmu menjadi motivasi penting hingga penelitian ini bisa diselesaikan.
5. Sahabat Konjep (Layla Rosyidah, Nurul Aulia Dewi, Puguh Mu'ammar Bramantyo, Yazmin Nur'Aini dan Yusuf Rafif Karback) terima kasih atas semangat, tawa, dan dukungan yang tak pernah putus selama proses penyusunan skripsi ini. Kebersamaan kalian tidak hanya menjadi penguat di masa-masa sulit, tetapi juga menjadi pengingat bahwa setiap perjuangan terasa lebih ringan ketika dijalani bersama.
6. Teman-teman TMJ angkatan 2021 yang selalu memberikan dukungan, ide-ide, serta saran yang membantu selama penelitian ini berlangsung.

Penulis menyadari bahwa karya tulis ini masih terdapat kekurangan dan keterbatasan. Oleh karena itu, adanya kritik dan saran yang bersifat membangun sebagai bahan evaluasi dan perbaikan di masa mendatang. Semoga karya tulis ini dapat memberikan manfaat bagi pembaca dan semua pihak yang membutuhkan.

Depok, 24 Juni 2025

Hary Alfajri

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama :	Hary Alfajri
NIM :	2107421013
Jurusan/Program Studi :	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Analisis Malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara Sandbox Custom, *Cuckoo Sandbox* , dan *Falcon Sandbox*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/ formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 24 Juni 2025
Yang Membuat Pernyataan

Hary Alfajri
NIM. 2107421013

ANALISIS MALWARE DENGAN METODE ANALISIS DINAMIS: PERBANDINGAN HASIL ANTARA SANDBOX CUSTOM, *CUCKOO SANDBOX* , DAN *FALCON SANDBOX*

ABSTRAK

Perkembangan teknologi yang pesat juga berdampak pada meningkatnya serangan siber, salah satunya melalui malware. Saat ini, banyak malware yang dibuat dengan teknik canggih agar bisa menghindari deteksi sistem keamanan. Untuk memahami cara kerja malware, analisis dinamis jadi salah satu metode yang sering digunakan karena bisa melihat langsung aktivitas malware di lingkungan yang aman atau sandbox. Dalam penelitian ini, membandingkan tiga jenis *sandbox*, yaitu *Cuckoo Sandbox, Falcon Sandbox,* dan *Custom Sandbox* yang dibuat sendiri.Pengujian dilakukan terhadap sembilan sampel malware dengan parameter yang sama, seperti aktivitas proses, file, registry, jaringan, memory dump, dan teknik evasive. Hasil pengujian menunjukkan bahwa *Custom Sandbox* berhasil mendeteksi 50 aktivitas mencurigakan, disusul *Cuckoo Sandbox* dengan 40 aktivitas, dan *Falcon Sandbox* dengan 34 aktivitas. Dari hasil tersebut, bisa dilihat bahwa *Custom Sandbox* memberikan hasil yang paling lengkap.Walaupun *Cuckoo* dan *Falcon* lebih praktis karena otomatis, *Custom Sandbox* lebih fleksibel dan mampu memberikan hasil analisis yang lebih detail. Jadi, meskipun butuh usaha lebih dalam prosesnya, pendekatan manual seperti *Custom Sandbox* bisa jadi alternatif yang efektif dalam mendeteksi dan memahami perilaku malware.

Kata Kunci: Malware, Analisis Dinamis, *Cuckoo Sandbox*, *Falcon Sandbox*, *Custom Sandbox*.

Daftar Isi

Daftar Gambar

Daftar Tabel

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi sekarang ini, manusia selalu bergantung pada teknologi, baik dalam aspek politik, sosial, pendidikan, maupun ekonomi. Di bidang ekonomi, teknologi memfasilitasi setidaknya dua metode pembayaran, yaitu dompet digital serta transfer bank online. Perkembangan teknologi memberikan sejumlah dampak positif bagi kehidupan manusia. Akan tetapi, bersamaan dengan kemajuan tersebut, ancaman keamanan siber meningkat secara signifikan, khususnya berupa *malware* yang semakin canggih serta kompleks. Perangkat lunak berbahaya, atau "*Malware (Malicious Software)*", secara aktif dirancang untuk merusak ke dalam sebuah sistem dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemiliknya seperti memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem yang dimaksud (Novansyah & Sutabri, 2023).

Serangan *malware* meningkat pesat dalam beberapa tahun terakhir, dikutip dari CNN Indonesia, Badan Siber dan Sandi Negara (BSSN) di awal tahun 2024 hingga bulan mei mencatat lebih dari 44 juta aktivitas *malware* yang mencakup 59, 76% dari total anomali trafik yang terjadi. Kerugian finansial yang diakibatkan oleh serangan *malware* menurut Kementerian Komunikasi dan Informatika (Kemenkominfo) yang dilaporkan secara global mencapai US$9, 5 triliun pada tahun 2024, diperkirakan akan meningkat menjadi US$10, 5 triliun pada tahun 2025. *Malware* modern telah berkembang dengan kemampuan untuk menyembunyikan kode berbahaya dan menghindari teknik analisis konvensional (Kumari & Verma, 2021).

Dalam analisis malware, salah satu pendekatan yang umum digunakan adalah analisis dinamis yang memungkinkan pengamatan langsung terhadap perilaku malware saat dieksekusi dalam lingkungan terkontrol, seperti sandbox. Framework yang digunakan seperti *Cuckoo Sandbox* dan *Falcon Sandbox*, yang mampu melakukan analisis otomatis terhadap berbagai aktivitas malware.Namun, kedua

framework tersebut masih memiliki keterbatasan dalam hal informasi yang diberikan serta fleksibilitas dalam pengaturan analisis.

Beberapa penelitian sebelumnya telah mengkaji penggunaan sandbox dalam analisis malware, namun mayoritas hanya berfokus pada satu atau dua jenis framework. Pada penelitian oleh Novansyah dan Sutabri (2023) menggunakan *Cuckoo Sandbox* untuk menganalisis malware *KMS-R@1n.exe*, namun tidak membandingkan efektivitas dengan sandbox lainnya. Penelitian oleh Wahidin et al. (2022) juga terbatas pada satu jenis malware dan belum menyentuh aspek fleksibilitas atau kedalaman analisis antar framework yang berbeda.

Dari permasalahan tersebut, dilakukan pengembangan *Custom Sandbox*, yaitu lingkungan analisis yang dirancang secara manual dengan memanfaatkan berbagai tools seperti Procmon, Wireshark, Process Explorer, Regshot, dan Volatility3. *Custom Sandbox* dimulai dari pembuatan lingkungan virtual, eksekusi malware, pemantauan aktivitas sistem, analisis memory dump, monitoring lalu lintas jaringan, serta pelaporan hasil. Dengan kombinasi ini, diharapkan dapat memberikan hasil yang lebih mendalam dan fleksibel.

Oleh karena itu, penelitian ini dilakukan untuk membandingkan hasil analisis dari tiga framework, yaitu *Custom Sandbox*, *Cuckoo Sandbox*, dan *Falcon Sandbox*, dengan menggunakan metode analisis dinamis. Perancangan *Custom Sandbox* sebagai alternatif framework yang lebih fleksibel yang dapat menghasilkan data analisis yang lebih mendalam dan dapat dikonfigurasi sesuai kebutuhan terhadap parameter yang diuji. Dengan adanya *Custom Sandbox* ini dapat meningkatkan efektivitas deteksi dan analisis malware dan dapat mengatasi keterbatasan yang ditemukan pada sandbox komersial seperti *Cuckoo Sandbox* dan *Falcon Sandbox*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, rumusan masalah yang dapat diambil pada analisis *malware* berbasis *framework Cuckoo Sandbox, Falcon Sandbox, dan Sandbox Custom* dengan metode analisis dinamis yaitu;

a. Bagaimana pengembangan *Custom Sandbox* untuk analisis malware berbasis analisis dinamis?
b. Bagaimana hasil perbandingan framework antara Cuckoo, Falcon dan *Custom Sandbox*?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini yaitu berfokus pada :

a. Penggunaan *framework Cuckoo Sandbox , Falcon Sandbox, dan sandbox* custom untuk analisis *malware*.
b. Jenis *malware* yang dianalisis yaitu Agentesla, AsyncRAT, BrainCipher, GrandCrab, Lumma, Remcos, ValleyRAT, WannaCry, dan Zeus.
c. Analisis yang digunakan hanya mencakup metode analisis dinamis saja.
d. Parameter yang diukur dari analisis tersebut yaitu, analisis proses, pencatatan aktivitas jaringan, *file operations*, *memory dump*, *registry change*, teknik evasive dan laporan hasil analisis.

1.4 Tujuan dan Manfaat

Tujuan:

a. Mengembangkan framework *Custom Sandbox* sebagai lingkungan analisis malware berbasis metode analisis dinamis, dengan memanfaatkan integrasi beberapa tools monitoring yang mampu memberikan hasil analisis lebih terperinci dan fleksibel.
b. Melakukan perbandingan antara *Cuckoo Sandbox, Falcon Sandbox,* dan *Custom Sandbox* dalam melakukan analisis terhadap sampel malware, dengan menilai efektivitas masing-masing framework berdasarkan parameter yang di analisis.

Manfaat:

a. Memberikan pemahaman tentang analisis *malware* berbasis *framework* dengan metode dinamis.
b. Memberikan alternatif solusi melalui pengembangan *Custom Sandbox* yang dapat disesuaikan dengan kebutuhan analisis, serta lebih mendalam dalam memantau perilaku malware dibandingkan framework otomatis yang telah ada.

1.5 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini adalah:

a. BAB 1 PENDAHULUAN

   Bab I berisi penjelasan mengenai latar belakang, rumusan, batasan, tujuan, dan manfaat analisis *malware* yang mendalam menggunakan *Custom Sandbox*, *Cuckoo Sandbox* dan *Falcon Sandbox* melalui metode analisis dinamis.

b. Bab II TINJAUAN PUSTAKA

   Bab II memaparkan beberapa landasan teori dan kajian ilmu yang relevan dengan sejumlah pokok pikiran utama dalam topik penelitian ini, serta pembahasan teori yang berhubungan dengan sumber yang terpercaya.

c. Bab III METODOLOGI PENELITIAN

   Bab III berisikan secara rinci rancangan penelitian, model atau kerangka kerja yang digunakan, metode analisis data, beserta jadwal pelaksanaan penelitian.

d. Bab IV HASIL DAN PEMBAHASAN

   Bab IV berisikan hasil dan pembahasan mengenai parameter pengujian *malware*, hasil pengujian dari ketiga *framework*, serta evaluasi dan analisis mendalam terhadap hasil yang diperoleh dan perbandingan efektivitas ketiga *framework* dalam analisis *malware*.

e. BAB V PENUTUP

   BAB V berisikan penjelasan mengenai hasil akhir dari penelitian berupa kesimpulan atas analisis yang dilakukan, serta saran untuk pengembangan penelitian lebih lanjut.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai " Analisis malware dengan Metode Analisis Dinamis: Perbandingan Hasil antara Sandbox Custom, *Cuckoo Sandbox* , dan *Falcon Sandbox*", dapat disimpulkan sebagai berikut:

1. Pengembangan *Custom Sandbox* dirancang untuk meningkatkan kemampuan dalam mendeteksi perilaku malawar secara fleksibel, terutama teknik evasive yang sering tidak terdeteksi oleh Sandbox otomatis.Dalam implementasinya, *Custom Sandbox* dibangun dengan mengintegrasikan beberapa tools yaitu process monitor tools yang digunakan untuk memantau aktivitas malwar terhadap file yang berjalan selama eksekusi, process explorer yang berfungsi untuk menganalisis proses aktif secara pada malware, termasuk parent-child relationship dan file executable yang mencurigakan. Regshot dimanfaatkan untuk melakukan melihat kondisi registry sebelum dan sesudah eksekusi malware, yang digunakan untuk melihat perubahan pada kunci registry yang dilakukan oleh malware, untuk menganalisis dump memory menggunakan tool Volatility3 dengan tujuan melihat aktivitas yang terjadi di dalam memori dan *injected code* serta wireshark digunakan untuk memantau dan menganalisis lalu lintas jaringan dan untuk mendeteksi upaya malware dalam melakukan koneksi ke server eksternal atau aktivitas komunikasi *Command and Control* (C2).
2. Dari hasil perbandingan ketiga framework menunjukan bahwa *Custom Sandbox* memiliki cakupan deteksi yang lebih luas terhadap enam parameter yang file operations, analisis proses, registry, memori, jaringan, dan teknik evasive.

5.2 Saran

Dari hasil analisis yang telah dilakukan, masih ditemukan beberapa kekurangan yang dapat menjadi bahan evaluasi kedepannya. Oleh karena itu, saran-saran

berikut yang dapat ditingkatkan untuk penelitian selanjutnya bisa menjadi lebih optimal dan menyeluruh.

1. Penelitian ini hanya membandingkan tiga framework, yaitu *Cuckoo Sandbox*, *Falcon Sandbox*, dan *Custom Sandbox*. Untuk penelitian selanjutnya, disarankan menambahkan framework sandbox lain agar hasil perbandingan lebih luas dan mendalam.
2. Jenis malware yang dianalisis masih terbatas pada sembilan sampel tertentu. Untuk memperkuat hasil, penelitian selanjutnya bisa mencoba menggunakan lebih banyak sampel malware dari berbagai kategori, seperti worm, spyware, keylogger, atau malware fileless.
3. Menambahkan parameter seperti penggunaan CPU dan memori saat malware berjalan, mekanisme *persistence*, atau analisis terhadap *command and control* (C2) server yang digunakan oleh malware.

Daftar Pustaka

Manoppo, V. A., Lumenta, A. S. M., & Karouw, S. D. S. (Tahun). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. Jurnal Teknik Elektro dan Komputer, vol. ?, no. ?, hal. ?-?. p-ISSN: 2301-8402, e-ISSN: 2685-368X.

Situmorang, S., Lubis, H., & Manullang, J. (2022). Analysis Of Malware Methods Using Dynamic Analysis In Detecting Malware. Jurnal Mantik, 6(2), 2639-2644.

Novansyah, H., & Sutabri, T. (2023). Analisis Malware dengan Metode Dinamik Menggunakan Framework *Cuckoo Sandbox*. Blantika: Multidisciplinary Journal, 1(2), 199-205.

Qomariah, N., & Alwi, M. (2020). Analisis Malware Hummingbad Dan Copycat Pada Metode Dynamic Analysis. Jurnal Teknologi dan Sistem Komputer, 8(2), 123-130.

Sari, D. P., & Rahman, A. (2023). Analisis Malware Menggunakan Metode Dynamic Analysis.

Alshahrani, A., & Alzahrani, A. (2020). Malware Detection Using Machine Learning Techniques: A Review. IEEE Access, 8, 9347415.

T. Sree Lakshmi, M. Govindarajan, and Asadi Sreenivasulu. (2020) Malware Detection Kit For *Malware* Analysis Of *Big Data*

Hidayat, R., & Rahman, A. (2021). Analisis Malware Menggunakan Metode Dynamic Analysis. Repositor: Jurnal Ilmiah Universitas Muhammadiyah Malang, 5(2), 123-130.

Alshahrani, A., & Alzahrani, A. (2023). A malware detection system using a hybrid approach of multi-heads attention-based control flow traces and image visualization.

Dener, M., Ok, G. & Orman, A**.,** 2022. Malware Detection Using Memory Analysis Data in Big Data Environment. *Applied Sciences*, 12(17), p.8604. [Online] Available at: https://doi.org/10.3390/app12178604 [Accessed 22 June 2025].

Ohello, S.P., 2023. *Pengembangan Teknik Evasion pada Malware Android untuk Menghindari Deteksi Anti-Malware Berbasis Signature dengan Menggunakan Obfuscation dan Dynamic Code Loading*. Tesis Magister, Institut Teknologi Bandung.

Preeti & Agrawal, A.K., 2022. A Comparative Analysis of Open Source Automated Malware Tools. In: *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, pp. 226–230.

Ali, S.F., Abdulrazzaq, M.R. and Gaata, M.T., 2025. *Learning Techniques-Based Malware Detection: A Comprehensive Review*. Mesopotamian Journal of Cybersecurity, 5(1), pp.273–300.

Aulawi, H., Utami, W. and Suhartanto, H., 2020. *Security Awareness Model in Higher Education: The Influence of Awareness on the Security Level*. Jurnal Teknologi dan Sistem Komputer, 8(4), pp.275–282.

Hoban, S., Bruford, M., D'Urban Jackson, J., Lopes-Ferreira, R., Heuertz, M., Hohenlohe, P.A., Paz-Vanegas, M., Segelbacher, G., Hunter, M.E., Geist, J. and Laikre, L., 2022. *Global genetic diversity status and trends: towards a suite of Essential Biodiversity Variables for genetic composition*. Biological Reviews, 97(5), pp.1731–1754.

Radoglou-Grammatikis, P., Zafeiropoulou, M., Atanasova, M., Zlatev, P., Giannakidou, S., Lagkas, T., Argyriou, V., Markakis, E.K., Moscholios, I. and Sarigiannidis, P., 2023. *False Data Injection Attacks Against High Voltage Transmission Systems*. In: 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Pafos, Cyprus, pp.324–329.

Samosir, A.S., Siregar, R.D. and Lubis, M., 2020. *Sistem Monitoring Tegangan dan Arus Berbasis Arduino Uno dan LabVIEW*. Jurnal Infotek (Jurnal Informatika dan Teknologi), 3(1), pp.35–53.

Somarriba, O., Perez Ramos, L.C., Zurutuza, U. and Uribeetxeberria, R., 2018. *Dynamic DNS Request Monitoring of Android Applications via Networking*. In: 2018 IEEE 38th Central America and Panama Convention (CONCAPAN XXXVIII). IEEE, pp.1–6.

Pillai, R., Thilakarathna, K. and Seneviratne, A., 2020. *A Comparative Analysis of Open Source Automated Malware Analysis Tools*. Future Generation Computer Systems, 111, pp. 1024–1037.

Liu, J., Yang, D., Lian, M. and Li, M., 2021. *Research on Intrusion Detection Based on Particle Swarm Optimization in IoT*. IEEE Access, 9, pp.38253–38270.

Carramiñana, D., Campaña, I., Bergesio, L., Bernardos, A.M. and Besada, J.A., 2021. Sensors and communication simulation for unmanned traffic management. Sensors, 21(3), p.927.

Chin, W.-L. and Isa, M., 2023. A Survey of Security Monitoring Systems for Host and Network. OIC-CERT Journal of Cyber Security, 2(1), pp.33–40.

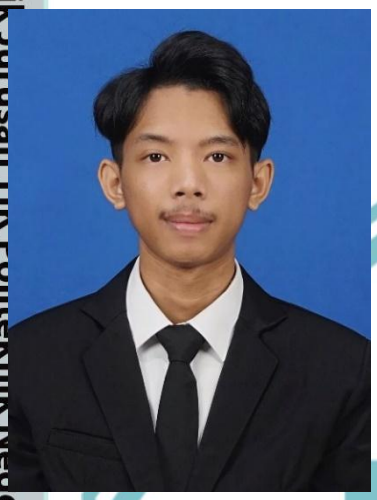
Johnson, A. and Haddad, R.J., 2021. Evading Signature-Based Antivirus Software Using Custom Reverse Shell Exploit. In: IEEE SoutheastCon 2021. IEEE, pp.1–6.

Koch, W. and Bestavros, A., 2016. Hiding from Automated Network Scans with Proofs of Identity. In: 2016 IEEE 4th Workshop on Hot Topics in Web Systems and Technologies (HotWeb). Washington, DC: IEEE, pp.66–71. doi:10.1109/HotWeb.2016.20.

IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Vancouver, BC, Canada, 18–22 June 2023. IEEE, pp.2797–2807. doi:10.1109/CVPR52729.2023.00283.

Aditya, I., Fitri, A.F. and Harjoko, A., 2021. Behavior Analysis and Monitoring (BAM) for Malware Detection and Mitigation in Windows Registry. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 5(2), pp.249–256.

Daftar Riwayat Hidup



Hary Alfajri

Lahir di Talawi, 11 September 2002, anak kedua dari tiga bersaudara. Telah lulus dari pendididkan formal SD Negeri 04 Rantih pada tahun 2015. Kemudian melanjutkan pendidikan menengah pertama di MTsN 2 Sawahlunto lulus. Pada tahun 2018 melanjutkan pendidikan atas di SMAN 2 Sawahlunto. Setelah itu pada tahun 2021, penulis berkesempatan untuk melanjutkan pendidikan tinggi di Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan jaringan.