Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

SLR Dengan Metode PRISMA: Perbandingan Sistem Keamanan Pada Sistem Operasi Windows Dan Linux

Meisya Amalia[1], Herbert Siregar[2]

[1 2]Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Ilmu Komputer, Universitas Pendidikan Indonesia, Bandung, Indonesia
Email: [1]meilia.23@upi.edu, [2]herbert@upi.edu
Email Penulis Korespondensi: herbert@upi.edu

Artikel Info :
Artikel History :
Submitted : 21- 6-2025
Accepted : 10-12-2025
Published : 30-04-2026

Kata Kunci:
Sistem_Keamanan; Windows; Linux; PRISMA; Sistem_Operasi

Abstrak−Penelitian ini bertujuan untuk melakukan perbandingan sistem keamanan antara sistem operasi Windows dan Linux melalui metode Systematic Literature Review (SLR) dengan pendekatan PRISMA. Studi ini menganalisis literatur dari tahun 2015 hingga 2025 yang diperoleh dari empat database akademik, yaitu Google Scholar, Scopus, IEEE Xplore, dan ScienceDirect. Hasil analisis menunjukkan bahwa Linux unggul dalam fleksibilitas konfigurasi keamanan, efisiensi sumber daya, dan respons terhadap ancaman siber melalui dukungan komunitas open-source. Sebaliknya, Windows menonjol dalam integrasi keamanan otomatis dan kemudahan penggunaan. Temuan ini menunjukkan bahwa efektivitas sistem keamanan sangat dipengaruhi oleh konteks penggunaan dan tingkat pemahaman pengguna terhadap sistem operasi yang digunakan. Dengan demikian, Linux cenderung lebih sesuai untuk lingkungan profesional yang membutuhkan kontrol sistem tinggi, sedangkan Windows lebih ramah bagi pengguna umum.

Keywords:
Security_System; Windows; Linux; PRISMA; Operating_ System

Abstract− *This study aims to compare the security systems of Windows and Linux operating systems using a Systematic Literature Review (SLR) method with the PRISMA approach. Literature from 2015 to 2025 was analyzed from four academic databases: Google Scholar, Scopus, IEEE Xplore, and ScienceDirect. The findings reveal that Linux is superior in security configuration flexibility, resource efficiency, and responsiveness to cyber threats through open-source community support. In contrast, Windows excels in integrated security automation and user-friendliness. These findings indicate that the effectiveness of security systems is highly influenced by the usage context and user understanding of the operating system. Therefore, Linux is more suitable for professional environments requiring high system control, while Windows is more user-friendly for general users..*

1. PENDAHULUAN

Sistem operasi merupakan komponen fundamental dalam ekosistem teknologi informasi yang menjadi landasan bagi operasional perangkat digital. Sistem operasi, yang menurut Silberschatz et al. [1] bertindak sebagai perantara vital antara pengguna dan perangkat keras komputer, dirancang untuk menyediakan lingkungan eksekusi program yang nyaman dan efisien sekaligus bertugas mengontrol alokasi sumber daya sistem secara adil. Lebih dari sekadar pengelola sumber daya, Whitman dan Mattord [2] menekankan bahwa dalam era digital modern, sistem operasi memegang peranan sentral dalam menjamin tiga pilar utama keamanan informasi (C.I.A. Triad), yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Kegagalan pada level sistem operasi dapat berakibat fatal, membuka celah bagi akses ilegal yang dapat mengompromikan seluruh data yang tersimpan di dalamnya Di antara berbagai sistem operasi yang tersedia, Windows dan Linux menjadi dua sistem yang paling banyak digunakan karena menawarkan karakteristik yang berbeda. Windows dikenal luas karena antarmuka pengguna yang intuitif dan dukungan aplikasi yang ekstensif, sedangkan Linux dikenal karena fleksibilitas dan tingkat keamanannya yang tinggi [3].

Meskipun demikian, perbandingan mendalam mengenai aspek keamanan dari kedua sistem ini masih belum banyak dilakukan secara sistematis dan menyeluruh. Mayoritas literatur terdahulu cenderung lebih berfokus pada pengukuran metrik kinerja komputasi (*performance benchmarking*) dan manajemen proses [4], [5], atau sekadar melakukan perbandingan fitur secara umum tanpa analisis kerentanan mendalam[6], serta menganalisis mekanisme pertahanan secara terisolasi pada satu *platform* saja tanpa melakukan komparasi *head-to-head*. Hal ini penting untuk dipahami, terutama dalam konteks meningkatnya ancaman siber yang menuntut sistem operasi mampu menyediakan perlindungan yang andal dan adaptif terhadap berbagai serangan.

Beberapa studi terkini menunjukkan bahwa efektivitas keamanan Windows dan Linux sering kali bergantung pada prioritas implementasinya, terutama terkait keseimbangan antara biaya dan kinerja. Zidan et al. [7] dalam analisis terbarunya menegaskan bahwa meskipun Windows menawarkan kemudahan penggunaan bagi pengguna umum, biaya lisensi dan kebutuhan spesifikasi perangkat keras yang tinggi menjadi kendala utama

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

dalam pemeliharaan jangka panjang. Sebaliknya, Linux dinilai lebih efisien secara ekonomi dan lebih aman untuk lingkungan yang memprioritaskan kustomisasi tanpa beban biaya lisensi. Temuan ini diperkuat oleh studi terbaru Ariza et al. [8] yang menyoroti perbedaan signifikan dalam manajemen memori antara kedua sistem operasi. Riset tersebut menunjukkan bahwa Linux memiliki mekanisme alokasi memori yang lebih optimal dan minim *overhead* dibandingkan Windows, yang cenderung membebani sumber daya akibat banyaknya proses latar belakang (*background services*). Hal ini mengindikasikan bahwa dalam konteks efisiensi operasional, Linux menawarkan stabilitas yang lebih baik untuk menjalankan protokol keamanan tanpa mengorbankan kinerja perangkat keras.

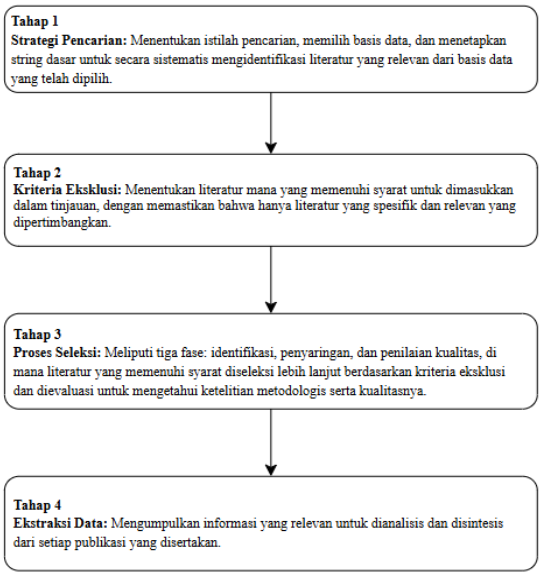
Namun, efisiensi teknis semata tidak menjamin keamanan total jika mengabaikan faktor manusia. Di Nocera dan Tempestini [9] menekankan bahwa aspek perilaku pengguna (*behavioral approach*) dan usabilitas sistem memainkan peran yang krusial. Sistem yang terlalu kompleks secara teknis seperti Linux berpotensi memicu kesalahan konfigurasi oleh pengguna awam, sedangkan sistem yang menawarkan otomatisasi tinggi seperti Windows dapat menurunkan kewaspadaan pengguna karena terciptanya rasa aman palsu (*false sense of security*). Berdasarkan kompleksitas tantangan tersebut, penelitian ini menggunakan metode *Systematic Literature Review* (SLR) dengan pendekatan *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) 2020. Pendekatan ini dipilih merujuk pada pedoman Page et al. [10], untuk mengidentifikasi, mengevaluasi, dan membandingkan sistem keamanan pada Windows dan Linux secara terstruktur berdasarkan literatur ilmiah terkini hingga tahun 2025.

Berdasarkan latar belakang tersebut, penelitian ini berusaha menjawab permasalahan utama terkait perbandingan efektivitas dan keandalan sistem keamanan antara Windows dan Linux, terutama dari aspek fitur keamanan, efisiensi penggunaan sumber daya, dan kerentanan terhadap ancaman siber. Selain menitikberatkan pada evaluasi teknis, penelitian ini juga memperluas cakupan analisisnya dengan mengkaji pengaruh faktor manusia, khususnya tingkat pemahaman pengguna, terhadap keberhasilan penerapan keamanan pada kedua sistem operasi tersebut. Penelitian ini mengajukan hipotesis bahwa terdapat perbedaan signifikan dalam pendekatan keamanan antara Windows dan Linux, di mana Linux dinilai lebih unggul dari sisi fleksibilitas dan efisiensi, sementara Windows menonjol dalam integrasi keamanan yang ramah pengguna.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Gambar 1 menunjukkan tahapan yang dilakukan dalam penelitian dimulai dari strategi pencarian hingga tahap ekstraksi data.



Gambar 1. Tahapan penelitian

Penelitian ini menggunakan metode Systematic Literature Review (SLR) dengan pendekatan PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Berdasarkan Gambar 1 penelitian ini terdiri dari empat tahapan utama, tahap pertama adalah strategi pencarian, di mana peneliti menentukan kata kunci seperti “Windows security system”, “Linux security system”, dan “comparison Windows Linux security” untuk menemukan literatur yang relevan melalui empat database akademik terkemuka: Google Scholar, Scopus, IEEE Xplore, dan ScienceDirect. Tahap ini bertujuan untuk mengidentifikasi artikel sebanyak mungkin yang berkaitan

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

dengan sistem keamanan pada Windows dan Linux. Setelah itu, tahap kedua adalah penerapan kriteria eksklusi, yang dilakukan untuk menyaring artikel yang tidak memenuhi syarat, seperti artikel yang tidak membandingkan kedua sistem operasi, bukan artikel ilmiah peer-reviewed, atau tidak berfokus pada aspek keamanan sistem operasi.

Tahap ketiga adalah proses seleksi yang melibatkan identifikasi, penyaringan, dan penilaian kualitas. Artikel yang lolos dari tahap eksklusi kemudian dievaluasi berdasarkan ketelitian metodologis dan relevansi terhadap fokus kajian. Penilaian kualitas dilakukan menggunakan kriteria tertentu, seperti kejelasan tujuan penelitian, kelengkapan metode, dan relevansi hasil. Tahap terakhir adalah ekstraksi data, yaitu mengumpulkan informasi penting dari artikel-artikel yang telah dipilih untuk dianalisis lebih lanjut. Informasi yang diekstrak meliputi fitur keamanan, efisiensi sistem, kerentanan terhadap ancaman siber, serta pengaruh pemahaman pengguna terhadap efektivitas sistem keamanan pada Windows dan Linux.

2.2 Strategi Pencarian

Tabel 1. memperlihatkan pencarian literatur yang dilakukan di beberapa database akademik terkemuka, yaitu Google Scholar, ScienceDirect, Scopus dan IEEE Xplore, dengan menggunakan kata kunci "Windows security system", "Linux security system", dan "comparison Windows Linux security" . Pencarian dilakukan untuk publikasi dalam rentang tahun 2015 hingga 2025.

Tabel 1. Jenis jenis database

Basis Data	URL
Google Scholar	https://scholar.google.com/
IEEE Xplore	https://ieeexplore.ieee.org/
ScienceDirect	https://www.sciencedirect.com/
Scopus	https://www.scopus.com/

Pemilihan keempat basis data tersebut didasarkan pada reputasinya yang tinggi dalam menyediakan literatur ilmiah yang berkualitas, khususnya di bidang ilmu komputer, teknologi informasi, dan keamanan sistem. Google Scholar dipilih karena cakupannya yang luas dan kemampuannya mengindeks berbagai jenis publikasi dari jurnal internasional maupun nasional. IEEE Xplore dan ScienceDirect merupakan platform yang secara khusus memuat artikel ilmiah hasil penelitian peer-reviewed dalam bidang teknik dan teknologi, yang sangat relevan dengan topik keamanan sistem operasi. Sementara itu, Scopus dikenal sebagai salah satu database bibliografis terbesar yang menawarkan abstrak dan kutipan dari literatur ilmiah dengan sistem penyaringan kualitas yang ketat. Penggunaan berbagai database ini bertujuan untuk memperoleh cakupan literatur yang komprehensif dan memastikan inklusi artikel dari berbagai perspektif penelitian, baik yang bersifat teoritis maupun praktis.

2.3 Kriteria Inklusi dan Eksklusi

Untuk memastikan kualitas dan relevansi artikel yang dianalisis dalam studi literatur ini, dilakukan proses seleksi berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Adapun kriteria inklusi dan eksklusi yang digunakan dalam studi ini adalah dapat dilihat pada Tabel 2 dan Tabel 3.

2.3.1 Kriteria Inklusi

Tabel 2. Kriteria inklusi dalam proses seleksi

No	Kriteria Inklusi
1.	Artikel yang membahas sistem Keamanan pada sistem operasi Windows dan Linux.
2.	Artikel yang bersifat komparatif antara Windows dan Linux.
3.	Artikel yang merupakan jurnal ilmiah atau prosiding konferensi *peer reviewed*.
4.	Artikel dalam bahasa Indonesia atau bahasa Inggris.

Berdasarkan rincian pada Tabel 2, penetapan kriteria inklusi ini bertujuan untuk menjamin validitas dan fokus penelitian. Penelitian ini memastikan bahwa data yang dikumpulkan memiliki standar kualitas ilmiah yang relevan dengan topik keamanan pada sistem operasi Windows dan Linux.

2.3.2 Kriteria Eksklusi

Tabel 3. Kriteria eksklusi dalam proses seleksi

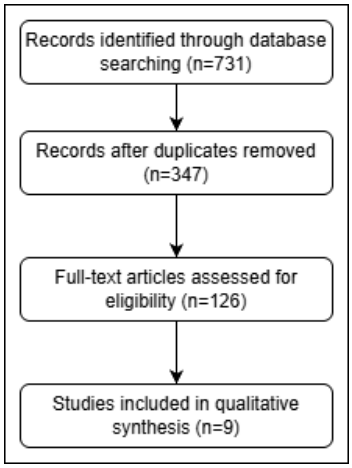
No	Kriteria Eksklusi
1.	Artikel berupa opini, blog, atau artikel populer non-akademik
2.	Duplikasi artikel yang sama pada database berbeda
3.	Artikel yang diterbitkan di luar rentang tahun yang ditentukan (sebelum tahun 2015)
4.	Artikel berupa poster, short communication, extended abstract, atau editorial.

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Penerapan kriteria eksklusi sebagaimana tercantum pada Tabel 3 berfungsi sebagai filter untuk mengeliminasi bias dan redundansi data. Kriteria ini menyaring sumber-sumber yang tidak memenuhi standar akademik, seperti artikel opini atau blog, serta memastikan kemutakhiran informasi dengan menghapus literatur yang terbit sebelum rentang waktu yang ditentukan, sehingga hasil analisis tetap relevan dengan perkembangan teknologi terkini

2.4 Proses Seleksi

Penelitian ini menggunakan metode studi literatur sistematis dengan pendekatan PRISMA untuk membandingkan sistem keamanan pada sistem operasi Windows dan Linux. Proses PRISMA di dalam penelitian dilakukan melalui tahapan pada Gambar 2.



Gambar 2. Tahapan seleksi menggunakan PRISMA flow diagram

Berdasarkan alur yang ditunjukkan pada Gambar 2, Sebanyak 731 artikel teridentifikasi pada tahap awal, yang kemudian disaring menjadi 347 setelah penghapusan duplikasi dan 126 artikel melalui penilaian teks lengkap, hingga akhirnya diperoleh 9 studi yang memenuhi kriteria untuk dianalisis secara kualitatif. Kesembilan artikel tersebut dianalisis secara kualitatif menggunakan teknik content analysis yang menitikberatkan pada aspek keamanan seperti manajemen akses, proteksi data, sistem deteksi intrusi, dan keandalan sistem. Hasil temuan kemudian nantinya akan disintesiskan dengan satu sama lain untuk mendapatkan gambaran komparatif yang komprehensif.

2.5 Quality Assessment

Untuk memastikan validitas dan reliabilitas studi yang akan dianalisis, penelitian ini menerapkan tahap penilaian kualitas (*Quality Assessment*) terhadap artikel-artikel yang telah melalui proses seleksi awal. Tahapan ini bertujuan untuk menyeleksi literatur yang tidak hanya relevan secara topik, tetapi juga memiliki standar metodologi yang baik dan dapat dipertanggungjawabkan. Penilaian dilakukan dengan mengevaluasi setiap artikel berdasarkan serangkaian daftar periksa (*checklist*) yang telah ditentukan. Adapun kriteria pertanyaan yang digunakan sebagai indikator penilaian kualitas dapat dilihat pada Tabel 4 berikut:

Tabel 4. Kriteria Quallity Assessment dalam bentuk pertanyaan

#	Kriteria (Pertanyaan)
QA1	Apakah artikel diterbitkan dalam rentang tahun 2015–2025 sesuai dengan cakupan literatur yang kamu tentukan?
QA2	Apakah artikel menyajikan data atau analisis yang relevan terkait keamanan sistem operasi?
QA3	Apakah artikel ditulis dalam Bahasa Indonesia atau Bahasa Inggris?
QA4	Apakah metode penelitian dijelaskan secara jelas dan dapat direplikasi?

Berdasarkan Tabel 4 di atas, proses penilaian dilakukan dengan memberikan respons "Ya" atau "Tidak" untuk setiap pertanyaan pada masing-masing artikel. Kriteria QA1 dan QA3 berperan sebagai filter administratif untuk menjamin kemutakhiran informasi (kebaruan) serta pemahaman bahasa. Sementara itu, kriteria QA2 dan QA4 difokuskan pada substansi konten dan ketetapan metodologi untuk menghindari bias dalam penarikan kesimpulan.

Hanya artikel yang mampu menjawab "Ya" pada seluruh atau sebagian besar kriteria kunci tersebut yang diikutsertakan (inklusi) ke dalam tahap sintesis data. Artikel yang tidak memenuhi standar kualitas ini, terutama

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

yang gagal memenuhi aspek relevansi (QA2) dan kejelasan metode (QA4), dieksklusi dari penelitian untuk menjaga integritas hasil komparasi sistem keamanan yang dilakukan.

3. HASIL DAN PEMBAHASAN

Tabel 5. Hasil Literature Review

Judul	Penulis (Tahun)	Metode	Temuan Utama	Kelebihan	Kekurangan
Literature Review Jurnal Memahami Faktor-Faktor yang Memengaruhi Popularitas Windows Dibanding kan Linux	Suci Maolia, Rahma Eka Aprilliana. (2024). [11]	Literature Review	Windows unggul dalam kompatibi-litas, antarmuka pengguna, dan dukungan software. Linux unggul dalam keamanan, fleksibilitas, kinerja, dan efektivitas biaya.	Menyajikan perbandingan komprehensif antara dua sistem operasi berdasarkan banyak aspek pengguna	Tidak mencantumkan data kuantitatif atau statistik pengguna secara eksplisit
Perbandi-ngan Kinerja Sistem Operasi Berbasis Server: Linux dan Windows Server	Yehezkiel Juandro Metta, Moh Jen Rumwokas , Elkin Rilvani. (2025). [12]	Eksperimen	Linux lebih unggul dalam efisiensi sumber daya dan stabilitas; Windows Server unggul dalam kemudahan penggunaan dan integrasi Microsoft	Menggunakan eksperimen langsung pada kondisi server yang seragam untuk validitas hasil	Fokus terbatas pada empat parameter saja, tidak membahas aspek biaya atau lisensi
Perbedaan Sistem Operasi Windows dengan Sistem Operasi Garuda Linux	Hilman Jihadi, Ghanistanti ono Dwi H, Amanda Arista, Jeremy Novaldo Parera. (2022). [13]	Deskriptif	Garuda Linux Memiliki fitur lengkap, tampilan modern, mampu menjalankan aplikasi Windows, Windows Lebih dikenal dan digunakan secara luas	Memberikan pengenalan terhadap sistem operasi lokal Garuda Linux dan Membanding-kannya dengan Windows dari sisi fitur dan hardware	Terbatas pada pemahaman pengguna mahasiswa; tidak ada pengujian kinerja langsung atau data kuantitatif
Analisa Kinerja Sistem Operasi Windows 10 dengan Linux Mint Mengguna-kan Aplikasi ZXT CAM, GNOME System Monitor	Tri Yusnanto, Sugeng Wahyudion o, Haryo Adiyatman Wicaksono. (2022). [14]	Eksperimen	Linux Mint Lebih unggul dalam hal waktu komputasi, efisiensi penggunaan sumber daya, dan jaringan dibandingkan Windows 10	Menggunakan aplikasi monitoring nyata (ZXT CAM & GNOME System Monitor) untuk pengukuran objektif	Hanya Membanding-kan dua distribusi spesifik; tidak mencakup aspek kompatibilitas atau UI/UX
Implement asi Sistem Keamanan Komputer Host Mengguna kan Sistem Operasi Fedora Linux	Samsoni, Aprilia Handayani,Elsa Apriliani, Zaman Padrisi, Rama Albin Sugiartha, Muhamad Arsyil Adzhim, Fariz Muhammad, Titis	Eksperimen	Menjelaskan bagaimana sistem operasi Fedora Linux digunakan untuk meningkat kan keamanan komputer host, termasuk fitur-fitur yang berkontribusi dalam	Fedora Linux dikenal sebagai sistem operasi yang stabil dan memiliki fitur keamanan bawaan yang kuat, serta dukungan komunitas	Bisa jadi ada tantangan dalam konfigurasi awal atau adaptasi bagi pengguna yang belum familiar dengan Linux.

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Judul	Penulis (Tahun)	Metode	Temuan Utama	Kelebihan	Kekurangan
	Wicaksono, Fajar Anggi Saputro. (2023). [15]		perlindungan data dan jaringan	yang luas.	
A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS	Adekotujo, A., Odumabo, A., Adedokun, A., & Aiyeniko, O. (2020). [6]	Perbandingan Berbasis Literatur	Setiap OS memiliki keunggulan berbeda, Windows unggul dalam kompatibilitas aplikasi, UNIX dan Linux unggul pada keamanan dan stabilitas, macOS unggul pada integrasi perangkat, Android dan iOS unggul pada pengalaman pengguna mobile.	Menyediakan perbandingan komprehensif antara enam sistem operasi dari berbagai kategori (desktop dan mobile).	Tidak melakukan uji eksperimental, analisis hanya berbasis literatur dan karakteristik umum OS
A systematic literature review on Windows malware detection: Techniques, research issues, and future	Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2024). [16]	Systematic Literature Review	Mengidentifikasi berbagai teknik deteksi malware Windows, termasuk signature-based, behavior-based, ML-based, serta mengungkap tantangan utama seperti obfuscation, polymorphism, dan kurangnya dataset representatif.	Menyajikan pemetaan komprehensif teknik deteksi malware dan memberikan arah penelitian masa depan yang jelas bagi peneliti keamanan siber.	Tidak membahas evaluasi kuantitatif antar metode secara mendalam dan belum menyediakan benchmark standar untuk pengujian praktis.
Security implications of running windows software on a Linux system using Wine: a malware analysis study	Duncan, R., & Schreuders, Z. C. (2019). [17]	Eksperimen	Malware Windows dapat berjalan pada Linux melalui Wine dengan tingkat keberhasilan bervariasi, beberapa malware tetap dapat mengeksekusi aksi berbahaya seperti file modification, process creation, dan registry-like changes. Wine tidak sepenuhnya mencegah eksekusi malware.	Memberikan analisis eksperimental nyata tentang bagaimana malware Windows berperilaku pada Wine, serta memberikan insight penting bagi pengguna Linux yang menjalankan aplikasi Windows.	Fokus terbatas pada jenis malware tertentu dan tidak mencakup seluruh varian modern; konfigurasi Wine yang digunakan tidak merepresentasikan semua skenario pengguna.
Linux Vs. Windows: A Comparison of Two Widely Used Platforms	Awan, M. T., & Khan, K. (2022). [18]	Perbandingan Berbasis Literatur	Linux memiliki keunggulan absolut dalam stabilitas server, keamanan cloud, dan efisiensi biaya karena sifat open-source; Windows mendominasi pasar desktop namun memiliki kelemahan dalam privasi data dan kerentanan terhadap bloatware.	Membahas relevansi OS dalam konteks infrastruktur modern (Cloud/Data Center) yang jarang disentuh studi desktop klasik	Analisis lebih berfokus pada arsitektur makro dan kebijakan lisensi, kurang membahas teknis deteksi malware secara spesifik.

Berdasarkan rangkuman literatur pada Tabel 5 di atas, terlihat adanya dikotomi yang jelas antara Windows dan Linux dalam hal orientasi desain dan prioritas keamanan. Studi-studi yang telah diseleksi, mulai dari hingga,

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

secara konsisten menunjukkan bahwa tidak ada sistem operasi yang unggul secara mutlak dalam seluruh parameter, keunggulan masing-masing sangat bergantung pada konteks penggunaannya.

3.1 Menjawab Pertanyaan Penelitian

Bagian ini menguraikan analisis mendalam untuk menjawab ketiga pertanyaan penelitian yang telah dirumuskan, dengan mensintesis temuan dari berbagai literatur mengenai fitur, faktor pengguna, dan pendekatan arsitektur sistem operasi.

3.1.1 RQ1: Apa saja fitur keamanan utama yang ditawarkan oleh sistem operasi Windows dan Linux, dan bagaimana efektivitasnya dalam menghadapi ancaman siber?

Berdasarkan tinjauan literatur, fitur keamanan utama pada Windows dan Linux memiliki pendekatan yang sangat berbeda yang berdampak langsung pada efektivitasnya. Maolia dan Aprilliana [11] menemukan bahwa kekuatan utama Windows terletak pada integrasi antarmuka dan kompatibilitas perangkat lunak yang luas, yang memfasilitasi penggunaan fitur keamanan otomatis bagi pengguna umum. Namun, dari sisi efisiensi teknis yang mendukung stabilitas keamanan, Metta et al. [12] membuktikan bahwa Linux Server jauh lebih unggul dalam manajemen sumber daya dibandingkan Windows Server, yang cenderung terbebani oleh layanan latar belakang.

Dalam hal antarmuka pengguna (UI) sebagai gerbang manajemen keamanan, Jihadi et al. [13] mencatat bahwa meskipun Linux (seperti Garuda Linux) telah memiliki tampilan modern, Windows masih memegang keunggulan dalam familiaritas. Kendati demikian, efektivitas teknis Linux dalam menjalankan proses komputasi terbukti lebih efisien, Yusnanto et al. [14] menunjukkan bahwa Linux Mint memiliki waktu komputasi yang lebih cepat dan penggunaan memori yang lebih stabil daripada Windows 10, yang secara tidak langsung meningkatkan ketersediaan sistem (availability) saat menghadapi beban tinggi.

Secara spesifik pada fitur pertahanan, Samsoni et al. [15] menyoroti efektivitas distro seperti Fedora Linux yang menyediakan fitur keamanan bawaan yang kuat (seperti SELinux) untuk melindungi host. Sebaliknya, efektivitas Windows sering kali diuji oleh volume serangan malware yang masif. Maniriho et al. [16] menjelaskan bahwa Windows sangat bergantung pada evolusi teknik deteksi malware (dari berbasis signature hingga perilaku), namun tetap menghadapi tantangan besar dari teknik pengaburan (obfuscation) oleh penyerang. Selain itu, Duncan dan Schreuders [17] menambahkan temuan kritis bahwa efektivitas keamanan Linux dapat menurun jika terjadi interoperabilitas; menjalankan aplikasi Windows di Linux menggunakan Wine terbukti masih memungkinkan eksekusi malware, menunjukkan bahwa fitur keamanan Linux tidak sepenuhnya kebal terhadap ancaman lintas platform.

3.1.2 RQ2: Apakah pendekatan open-source yang diterapkan oleh Linux lebih efektif dalam meningkatkan keamanan sistem dibandingkan pendekatan tertutup pada Windows?

Pendekatan *open-source* yang menjadi fondasi utama sistem operasi Linux menunjukkan keunggulan efektivitas yang sangat nyata dan signifikan, khususnya ketika diterapkan dalam konteks infrastruktur teknologi yang kompleks serta kemampuan adaptasi terhadap perubahan kebutuhan sistem. Dalam analisis komparatifnya, Awan dan Khan [18] secara tegas menegaskan bahwa di dalam ekosistem lingkungan *cloud computing* dan pusat data modern (*data center*), Linux memegang dominasi dan keunggulan absolut dibandingkan Windows. Keunggulan struktural ini utamanya didorong oleh sifat keterbukaan kode (*open-source*) yang memungkinkan dilakukannya audit keamanan secara masif, transparan, dan berkelanjutan oleh komunitas pengembang global. Partisipasi komunitas yang luas ini tidak hanya mempercepat deteksi kerentanan, tetapi juga menjamin stabilitas sistem yang lebih tinggi, yang merupakan elemen vital bagi keberlangsungan layanan digital modern.

Lebih jauh lagi, transparansi kode sumber ini tidak hanya menawarkan visibilitas, tetapi juga menjadi kunci yang memungkinkan penerapan metode pengamanan yang jauh lebih mendalam dan spesifik sesuai kebutuhan organisasi. Hal ini dibuktikan secara teknis oleh penelitian Prabowo et al. [19], yang menunjukkan bahwa efektivitas keamanan pada sistem Linux dapat dimaksimalkan hingga potensi tertingginya melalui penerapan metode *hardening* yang berlapis dan komprehensif. Mekanisme pengerasan sistem ini dapat dikonfigurasi secara granular dan presisi, mulai dari perlindungan pada Layer 1 (aspek fisik) hingga Layer 7 (lapisan aplikasi). Fleksibilitas konfigurasi tingkat tinggi seperti ini merupakan kemampuan yang sangat sulit, bahkan hampir mustahil, dicapai pada sistem dengan arsitektur tertutup (*closed-source*) seperti Windows, yang secara desain membatasi hak akses pengguna maupun administrator untuk memodifikasi atau mengaudit inti *kernel* sistem secara langsung demi alasan properti intelektual.

Sebagai sintesis akhir dalam membandingkan efektivitas kedua pendekatan arsitektur ini, Yunianto dan Adhiyarta [20] dalam tinjauan literatur mereka merangkum sebuah kesimpulan krusial: pendekatan *open-source* yang ditawarkan Linux terbukti jauh lebih efektif dan relevan bagi lingkungan operasional yang memprioritaskan kontrol penuh atas sistem, transparansi proses, serta efisiensi biaya lisensi dalam jangka panjang. Di sisi lain, pendekatan tertutup yang diusung oleh Windows, meskipun menawarkan kemudahan dalam hal integrasi

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

ekosistem aplikasi yang seragam, sering kali menghadapi kendala signifikan dalam aspek ketangkasan keamanan. Sistem tertutup cenderung tertinggal dalam kecepatan penambalan celah keamanan (*patching*) karena proses mitigasi tersebut bergantung sepenuhnya pada siklus rilis dan sumber daya dari satu vendor tunggal, berbeda dengan mekanisme respons yang jauh lebih cepat dan kolaboratif yang dimiliki oleh komunitas *open-source* dalam menutup celah kerentanan baru.

3.1.3 RQ3: Bagaimana pengaruh tingkat pemahaman pengguna terhadap efektivitas sistem keamanan pada Windows dan Linux?

Faktor pengguna terbukti menjadi variabel penentu yang signifikan dalam efektivitas keamanan kedua sistem operasi. Ilhamdi dan Kunang [21] mengungkapkan melalui analisis forensik bahwa pada sistem Windows, banyak insiden keamanan terjadi karena ketidakmampuan pengguna mendeteksi *malware* yang menyembunyikan diri di balik proses sistem yang sah. Hal ini menunjukkan bahwa sistem keamanan otomatis pada Windows sering kali memberikan rasa aman palsu jika tidak dibarengi dengan pemahaman pengguna.

Perbedaan kurva pembelajaran juga mempengaruhi profil risiko. Abdul et al. [22] menyimpulkan bahwa meskipun Linux dan MacOS secara inheren lebih aman dari virus dibanding Windows, keduanya menuntut tingkat pemahaman teknis yang tinggi; pengguna yang tidak kompeten cenderung kesulitan mengamankan sistem Linux secara efektif. Untuk mengatasi celah pemahaman pada pengguna Windows, Fadil [23] menyarankan strategi pengembangan keamanan terpadu yang tidak hanya berfokus pada *software* antivirus, tetapi juga mencakup kebijakan edukasi pengguna untuk memitigasi ancaman siber secara proaktif.

Risiko akibat kurangnya pemahaman pada Linux terlihat jelas dalam administrasi server. Zahra et al. [24] mendemonstrasikan bahwa layanan SSH pada server Linux sangat rentan terhadap serangan *brute force* menggunakan *tools* seperti Hydra jika administrator lalai melakukan konfigurasi dasar (seperti pembatasan *login*). Temuan ini menegaskan bahwa efektivitas keamanan Linux sangat bergantung pada *skill* pengguna dalam melakukan konfigurasi, berbeda dengan Windows yang lebih mengandalkan proteksi *default* vendor.

4. KESIMPULAN

Berdasarkan hasil SLR yang komprehensif, penelitian ini menyimpulkan bahwa tidak ada sistem operasi yang memegang supremasi keamanan mutlak yang terjadi adalah dikotomi fundamental antara kenyamanan penggunaan dan ketangguhan arsitektur. Windows secara konsisten unggul dalam integrasi sistem dan otomatisasi pertahanan yang ramah pengguna, menjadikannya standar produktivitas global. Namun, dominasi ini menciptakan paradoks di mana Windows menjadi target utama serangan siber. Kompleksitas malware modern yang menyerang platform ini menuntut mekanisme deteksi hibrida yang berat, yang terbukti membebani sumber daya komputasi dan menurunkan efisiensi sistem pada perangkat keras terbatas.

Sebaliknya, Linux menunjukkan superioritas tak terbantahkan dalam aspek efisiensi sumber daya, stabilitas, dan transparansi kode (*open-source*), menjadikannya fondasi utama bagi infrastruktur kritis modern seperti cloud computing dan pusat data. Kendati demikian, penelitian ini mematahkan mitos bahwa Linux sepenuhnya kebal terhadap ancaman. Risiko keamanan pada Linux bergeser dari kerentanan default menuju risiko interoperabilitas dan kesalahan konfigurasi. Penggunaan lapisan kompatibilitas untuk menjalankan aplikasi lintas platform terbukti dapat membuka celah keamanan fatal, menegaskan bahwa isolasi lingkungan adalah kunci pertahanan Linux.

Pada akhirnya, efektivitas sistem keamanan sangat bergantung pada faktor manusia. Tantangan terbesar Linux terletak pada kurva pembelajaran yang curam yang rentan terhadap kesalahan konfigurasi manual, sedangkan tantangan Windows adalah budaya ketergantungan pengguna pada otomatisasi yang menurunkan kewaspadaan. Oleh karena itu, pemilihan sistem operasi harus didasarkan pada konteks strategis: Linux adalah pilihan terbaik untuk infrastruktur yang membutuhkan kontrol penuh dan efisiensi tinggi, sementara Windows tetap relevan untuk lingkungan pengguna akhir yang memprioritaskan kompatibilitas ekosistem, dengan catatan bahwa peningkatan literasi keamanan digital merupakan elemen pertahanan yang wajib bagi kedua platform.

REFERENCES

[1] S. Abraham, P. B. Galvin, and G. Greg, “Operating System Concepts (10th ed.),” vol. 11, no. 1, pp. 1–14, 2022, [Online]. Available: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

[2] M. E. Whitman and H. J. Mattord, “Principles of Information Security,” *Cengage Learn.*, no. September, p. 11, 2018, [Online]. Available: www.cengage.com.

[3] I. H. S. Dwinanto, "Implementasi keamanan komputer pada aspek confidentiality, integrity, availability (cia) menggunakan tools lynis audit system," *J. Maklumatika*, vol. 8, no. 1, pp. 35–46, 2021.

[4] Ghufron Malik, Kholid Wahyudi, Febri Tri Arie Sakti, Abdul Ghofar, and Abdul Halim Anshor, "Analisa Perbandingan Manajemen Proses Multitasking pada Sistem Operasi Windows dan Linux," *J. Tek. Mesin, Ind. Elektro dan Inform.*, vol. 3, no. 4, pp. 190–199, 2024, doi: 10.55606/jtmei.v3i4.4538.

[5] W. C. Fan, C. S. Wong, W. K. Lee, and S. O. Hwang, "Comparison of interactivity performance of linux CFS and windows 10 CPU schedulers," *Proc. - 2020 Int. Conf. Green Hum. Inf. Technol. ICGHIT 2020*, pp. 31–34, 2020, doi: 10.1109/ICGHIT49656.2020.00014.

[6] A. Adekotujo, A. Odumabo, A. Adedokun, and O. Aiyeniko, "A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS," *Int. J. Comput. Appl.*, vol. 176, no. 39, pp. 16–23, 2020, doi: 10.5120/ijca2020920494.

[7] Zidan, R. Al Fajar, and A. Lestari, "Analisis Perbandingan Sistem Operasi Windows 11 dan Linux Ubuntu Menggunakan Metode Studi Literatur (Studi Kasus : Kinerja Sistem, Keamanan dan Biaya)," *Bitwise J. Teknol. Inf. dan Komputasi*, vol. 1, no. 2, pp. 74–82, 2025, [Online]. Available: https://jurnal-bitwise.org/index.php/bitwise/article/view/20

[8] R. Ariza, M. Reza Maulana, and E. Rilvani, "Perbandingan Manajemen Memori pada Sistem Operasi Windows dan Linux," *J. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 1, pp. 115–128, 2024, doi: 10.59581/jusiik-widyakarya.v3i1.4471.

[9] F. Di Nocera and G. Tempestini, "Getting Rid of the Usability/Security Trade-Off: A Behavioral Approach," *J. Cybersecurity Priv.*, vol. 2, no. 2, pp. 245–256, 2022, doi: 10.3390/jcp2020013.

[10] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Bmj*, vol. 372, 2021, doi: 10.1136/bmj.n71.

[11] S. Maolia and Rahma Eka Aprilliana, "Literature review jurnal memahami faktor-faktor yang mempengaruhi popularitas windows dibandingkan linux," *J. Mhs. Tek. Inform.*, vol. 3, no. 1, pp. 96–101, 2024, doi: 10.35473/jamastika.v3i1.2791.

[12] Y. J. Metta, M. J. Rumwokas, and E. Rilvani, "Perbandingan kinerja sistem operasi berbasis server: Linux dan windows server," *J. Cybern. Inov.*, vol. 9, no. 1, 2025.

[13] H. Jihadi, G. D. H, and A. Arista, "Perbedaan sistem operasi windows dengan sistem operasi garuda linux," *J. Sist. Inf. Bisnis*, vol. 3, no. 2, pp. 0–5, 2022, [Online]. Available: https://ejournal-ibik57.ac.id/index.php/junsibi/article/view/555/286

[14] T. Yusnanto, S. Wahyudiono, and H. A. Wicaksono, "Analisa kinerja sistem operasi windows 10 dengan linux mint menggunakan aplikasi zxt cam, gnome system monitor," *SENTRI J. Ris. Ilm.*, vol. 1, no. 2, pp. 288–296, 2022, doi: 10.55681/sentri.v1i2.210.

[15] I. D. Christ Evvert Lisangan, "Implementasi sistem keamanan komputer host menggunakan sistem operasi fedora linux," *Maklumatika*, vol. 7, no. 2, pp. 109–118, 2021, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/105/110

[16] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A systematic literature review on Windows malware detection: Techniques, research issues, and future directions," *J. Syst. Softw.*, vol. 209, 2024, doi: 10.1016/j.jss.2023.111921.

[17] R. Duncan and Z. C. Schreuders, "Security implications of running windows software on a Linux system using Wine: a malware analysis study," *J. Comput. Virol. Hacking Tech.*, vol. 15, no. 1, pp. 39–60, 2019, doi: 10.1007/s11416-018-0319-9.

[18] M. T. Awan, "Linux vs. Windows: A Comparison of Two Widely Used Platforms," *J. Comput. Sci. Technol. Stud.*, vol. 4, no. 1, pp. 41–53, 2022, doi: 10.32996/jcsts.2022.4.1.4.

[19] M. A. Prabowo, U. Darusalam, and S. Ningsih, "Perancangan Keamanan Server Linux Dengan Metode Hardening Pada Layer 1 dan Layer 7," *J. Media Inform. Budidarma*, vol. 4, no. 3, p. 591, 2020, doi: 10.30865/mib.v4i3.2157.

[20] I. Yunianto and K. Adhiyarta, "Jurnal Review: Perbandingan Sistem Operasi Linux Dengan Sistem Operasi Windows," *JUPITER J. Comput. Inf. Technol.*, vol. 1, no. 1, pp. 1–7, 2020, doi: 10.53990/jupiter.v1i1.3.

[21] Y. Ilhamdi and Y. N. Kunang, "Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik," *Bina Darma Conf. Comput. Sci.*, pp. 256–264, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124

[22] D. F. Abdul, M. I. Budiman, and T. Kurniawan, "Analisis sistem keamanan sistem operasi (Windows, Linux, MacOS)," *Comput. \& Secur. March*, 2019.

[23] Sarvina Sari Ahmad Fadil, "Strategi pengembangan sistem keamanan terpadu untuk melindungi sistem operasi windows dari ancaman cyber," *Router J. Tek. Inform. dan Terap.*, vol. 2, no. 3, pp. 122–136, 2024, doi: 10.62951/router.v2i3.154.

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

[24] D. R. Az Zahra, F. P. Ilham, H. N. Ramdhani, and A. Setiawan, "Penerapan dan Pengujian Keamanan SSH Pada Server Linux menggunakan Hydra," *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 10, 2024, doi: 10.47134/pjise.v1i3.2627.