Jurnal Sistem Dan Teknologi Informasi (JSTI)

https://journalversa.com/s/index.php/jsti Vol. 07, No. 1 Februari 2025

EVALUASI KEAMANAN SISTEM OPERASI LINUX DARI SERANGAN MALWARE

Muhamad Jati Wasesa[1]
Email: muh.jati@mhs.pelitabangsa.ac.id

Hardi Wirkan[2]
Email: wirkanhardi@gmail.com

Elkin Rilvani[3]
Email: elkin.rilvani@pelitabangsa.ac.id

[1,2,3]Universitas Pelita Bangsa

ABSTRAK

Keamanan menjadi salah satu aspek terpenting dalam menjaga integritas dan kerahasiaan data. Sistem operasi Linux, yang dikenal dengan kestabilan dan keamanannya, sering dipilih sebagai platform untuk berbagai aplikasi server. Namun, meskipun Linux memiliki berbagai fitur keamanan bawaan, ancaman malware tetap menjadi tantangan serius. Jurnal ini bertujuan untuk menganalisis sistem keamanan jaringan pada sistem operasi Linux terhadap serangan malware, dengan fokus pada teknik-teknik pencegahan dan deteksi yang efektif. Penelitian ini menggunakan data dan statistik terkini untuk menggambarkan prevalensi serangan malware di lingkungan Linux serta mengeksplorasi pendekatan yang dapat diambil untuk meningkatkan keamanan. Melalui studi kasus dan analisis literatur, jurnal ini memberikan wawasan mendalam mengenai tantangan dan solusi dalam melindungi jaringan Linux dari ancaman malware.

Kata Kunci: Linux, Jaringan, Malware.

ABSTRACT

Security is one of the most important aspects in maintaining data integrity and confidentiality. The Linux operating system, which is known for its stability and security, is often chosen as a platform for various server applications. However, even though Linux has a variety of built-in security features, malware threats remain a serious challenge. This journal aims to analyze the network security system on the Linux operating system against malware attacks, with a focus on effective prevention and detection techniques. This research uses the latest data and statistics to illustrate the prevalence of malware attacks in Linux environments and explore approaches that can be taken to improve security. Through case studies and literature analysis, this journal provides in-depth insight into the challenges and solutions in protecting Linux networks from malware

threats.

Keywords: *Linux, Network, Malware.*

1. PENDAHULUAN

keamanan jaringan menjadi salah satu aspek yang sangat penting, terutama dalam konteks sistem operasi Linux (Maulana, 2022). Linux, dengan arsitektur open-source-nya, menawarkan fleksibilitas dan kontrol yang lebih besar bagi pengguna, namun juga menghadapi tantangan serius terkait serangan malware (Yunanri.W, 2024). Menurut laporan dari Cybersecurity & Infrastructure Security Agency (CISA), serangan terhadap sistem berbasis Linux meningkat sebesar 50% dalam dua tahun terakhir, menunjukkan bahwa ancaman ini tidak dapat diabaikan (Nissim, N. (2021).

Malware, yang mencakup berbagai bentuk perangkat lunak berbahaya seperti virus, worm, dan ransomware, dapat menyebabkan kerusakan signifikan pada sistem dan jaringan(Wiwin Sulistyo, 2023). Sebuah studi oleh Maulana et al. (2022) menunjukkan bahwa penerapan filter proxy server dapat mengurangi penyebaran malware hingga 30% dalam lingkungan jaringan tertentu. Ini menunjukkan bahwa langkah-langkah pencegahan yang tepat dapat mengurangi risiko serangan dan melindungi data sensitif.

Bagaimana cara mengamankan sistem Linux dari serangan malware. Untuk mengamankan sistem Linux dari serangan malware, diperlukan pendekatan yang menyeluruh dan terintegrasi, mengingat meskipun Linux dikenal sebagai sistem operasi yang stabil dan aman, ia tetap rentan terhadap berbagai ancaman. Penggunaan Perangkat Lunak Antivirus: Meskipun Linux memiliki reputasi lebih baik dalam hal keamanan, penggunaan perangkat lunak antivirus tetap diperlukan (Nissim, 2021). Perangkat lunak ini dapat membantu mendeteksi dan menghapus malware yang mungkin berhasil masuk ke dalam sistem (Maulana, 2022). Pilihlah antivirus yang dirancang khusus untuk Linux agar dapat memberikan perlindungan maksimal.(M Hatta, 2022).

Implementasi Firewall: Menggunakan firewall untuk mengontrol lalu lintas jaringan adalah langkah penting dalam melindungi sistem dari serangan eksternal. Firewall dapat dikonfigurasi untuk memblokir akses tidak sah dan hanya memperbolehkan koneksi dari sumber yang terpercaya (Sumijan, 2024).

Penelitian ini bertujuan untuk mengevaluasi pada keamanan sistem linux ubuntu,

dampaknya terhadap kinerja sistem operasi linux ubuntu. Sistem operasi Linux, meskipun dikenal dengan keamanannya yang lebih baik dibandingkan dengan sistem operasi lain, tetap rentan terhadap serangan malware. Misalnya, laporan oleh Panker dan Nissim (2021) mengungkapkan bahwa banyak serangan malware di lingkungan cloud Linux memanfaatkan celah keamanan yang ada dalam konfigurasi sistem. Oleh karena itu, penting untuk memahami bagaimana malware dapat menyerang dan bagaimana sistem keamanan dapat dioptimalkan untuk melindungi jaringan.

Dalam konteks ini, analisis sistem keamanan jaringan pada Linux perlu dilakukan dengan pendekatan yang komprehensif. Penelitian oleh Widyatono dan Sulistyo (2023) menunjukkan bahwa pemodelan Intrusion Prevention System (IPS) dapat meningkatkan deteksi dan pencegahan penyebaran malware, dengan tingkat efektivitas mencapai 85%. Ini menunjukkan bahwa penggunaan teknologi deteksi yang canggih sangat penting untuk mempertahankan integritas sistem.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam analisa sistem keamanan jaringan pada sistem operasi Linux terhadap serangan malware melibatkan beberapa langkah yang sistematis. Berikut adalah flowchart yang menggambarkan proses penelitian ini.

Gambar 1. Alur Penelitian

Flowchart yang menggambarkan proses penelitian ini

1. **Identifikasi Masalah** : Mengidentifikasi jenis serangan malware yang umum terjadi pada sistem operasi Linux.
2. **Pengumpulan Data** : Mengumpulkan data dari berbagai sumber, termasuk literatur, studi kasus, dan data statistik mengenai serangan malware.
3. **Analisis Data** : Melakukan analisis terhadap data yang telah dikumpulkan untuk memahami pola serangan dan metode pencegahan yang efektif.
4. **Triangulasi**: Melakukan penggabungan berbagai sumber data, seperti literatur, studi kasus, dan wawancara untuk memastikan validitas dan keakuratan dalam sistem keamanan jaringan berbasis Linux guna mencegah serangan malware.
5. **Kesimpulan** : Menyimpulkan hasil analisis berdasarkan data yang telah dikumpulkan, memastikan efektivitas langkah-langkah yang diusulkan dalam mencegah serangan malware pada sistem operasi Linux, serta memberikan rekomendasi untuk pengembangan keamanan jaringan di masa depan

3. LITERATURE REVIEW

Tabel 1. Literature Review

Judul jurnal	Penulis	Tahun	Ringkasan	Penyelesaian
Pemodelan Intrusion Prevention System untuk Pendeteksi dan Pencegahan Penyebaran Malware Menggunakan Wazuh	Panker, Tomer; Nissim, Nir	2021	Membahas pentingnya IPS dalam mendeteksi dan mencegah serangan malware secara real-time, serta fitur Wazuh seperti Security Analytics dan Intrusion Prevention.	Menggunakan Wazuh untuk memantau lalu lintas jaringan dan memberikan peringatan real-time dengan menganalisis pola ancaman.
Analisis Perbandingan Optimalisasi Port Knocking dan Honeypot dengan IPTables	Dermawan, Anjun; Yuhandri	2024	Menilai efektivitas kombinasi Port Knocking dan Honeypot untuk meningkatkan keamanan server	Kombinasi Port Knocking dan Honeypot dengan IPTables, memberikan bukti empiris

			terhadap serangan DoS dan Brute Force, dengan pengurangan signifikan dalam penggunaan sumber daya.	berupa data kuantitatif untuk mengamankan port dan mengurangi penggunaan CPU serta memori.
Leveraging Malicious Behavior Traces from Volatile Memory Using Machine Learning Methods	Panker, Tomer; Nissim, Nir	2021	Kerangka kerja berbasis machine learning untuk mendeteksi malware tidak dikenal di lingkungan cloud Linux. Menganalisis memori volatil untuk mendeteksi ancaman baru dengan tingkat positif palsu yang rendah.	Memanfaatkan 171 fitur informatif dari dump memori volatil dengan algoritma machine learning untuk membedakan aktivitas jinak dan berbahaya.
Analisa Penerapan Filtering Proxy Server pada Keamanan Jaringan Komputer	Maulana, R; Hatta, M	2022	Mengurangi penyebaran malware melalui server proxy penyaringan pada lembaga pendidikan. Penelitian menggunakan Linux Ubuntu dan perangkat lunak Squid sebagai referensi untuk proyek keamanan jaringan.	Implementasi siklus PPDIOO (Persiapkan, Rencanakan, Desain, Implementasi, Operasi, Optimalkan) untuk menyaring lalu lintas jaringan dan membatasi akses ke situs web berbahaya.

Deteksi Serangan Malware pada Web Aplikasi Menggunakan Metode Malware Analis Dinamis dan Statis	Yunanri, W; Fitriana, Y.B	2024	Mengembangkan model yang menggabungkan analisis dinamis dan statis untuk mendeteksi malware dalam aplikasi web, dengan tingkat akurasi tinggi (99,8%) dan tingkat positif palsu minimal.	Menggunakan alat seperti Wireshark untuk analisis jaringan dan Regshot untuk pemantauan registri. Model jaringan saraf digunakan untuk mendeteksi file PE dalam aplikasi web.
Identification of Toolchains Used to Build IoT Malware	Akabane, Shu; Okamoto, Takeshi	2021	Identifikasi toolchain untuk malware IoT di berbagai arsitektur. Studi ini menyoroti dominasi penggunaan perpustakaan UClibC dalam malware IoT.	Menggunakan pola fungsi pustaka dan aturan YARA untuk mengidentifikasi toolchain yang digunakan dalam malware IoT, termasuk generasi pola khusus untuk beberapa arsitektur.

Pengantar Keamanan Jaringan pada Linux

Keamanan jaringan merupakan aspek penting dalam pengelolaan sistem operasi, terutama pada Linux yang dikenal sebagai sistem operasi yang aman dan stabil. Namun, meskipun Linux memiliki reputasi yang baik, bukan berarti ia kebal terhadap serangan malware (Syafrinal, 2021). Berdasarkan laporan dari Panker dan Nissim (2021), serangan malware pada lingkungan cloud yang menggunakan Linux meningkat seiring dengan berkembangnya teknologi. Statistik menunjukkan bahwa sekitar 30% dari semua serangan malware yang dilaporkan terjadi pada sistem berbasis Linux, menunjukkan perlunya peningkatan keamanan yang lebih baik (Akabane & Okamoto, 2021).

Sistem operasi Linux sering digunakan dalam perangkat komputer, menjadikannya

target yang menarik bagi penyerang. Malware yang ditujukan untuk Linux dapat bervariasi dari virus, worm, hingga ransomware, masing-masing dengan teknik penyebaran yang berbeda (Nissim, 2021). Sebagai contoh, ransomware Linux baru-baru ini menyerang server web, mengenkripsi file dan meminta tebusan untuk mengembalikannya (Widyatono & Sulistyo, 2023).

Keberadaan berbagai distribusi Linux juga menambah kompleksitas dalam hal keamanan. Setiap distribusi memiliki konfigurasi dan kebijakan keamanan yang berbeda, yang dapat menjadi celah jika tidak dikelola dengan baik. Maulana et al. (2022) mencatat bahwa penerapan filtering proxy server dapat membantu meminimalisir penyebaran malware dengan menyaring konten berbahaya sebelum mencapai pengguna. Ini menunjukkan pentingnya pendekatan multi-layer dalam keamanan jaringan Linux.

Dalam konteks ini, penting untuk menerapkan sistem deteksi intrusi (IDS) seperti Snort, yang dapat membantu mendeteksi dan merespons serangan malware secara real-time (Sumijan, 2024). Dengan memanfaatkan teknologi ini, administrator jaringan dapat mengidentifikasi perilaku mencurigakan dan mengambil tindakan pencegahan yang diperlukan.

Secara keseluruhan, meskipun Linux memiliki banyak keunggulan dalam hal keamanan, ancaman malware tetap ada. Oleh karena itu, pendekatan yang komprehensif dan terintegrasi dalam keamanan jaringan sangat diperlukan untuk melindungi sistem berbasis Linux.

Tipe-Tipe Malware yang Menyerang Linux

Serangan malware pada sistem operasi Linux dapat dikategorikan ke dalam beberapa tipe, masing-masing dengan metode penyebaran dan dampak yang berbeda. Salah satu tipe yang paling umum adalah virus, yang dapat menyebar melalui file yang terinfeksi dan mengganggu fungsi sistem (Yunanri.W, 2024). Berdasarkan penelitian oleh Dermawan et al. (2024), virus yang ditujukan untuk Linux sering kali menyusup melalui aplikasi yang diunduh dari sumber tidak resmi, yang menunjukkan pentingnya pengawasan dalam pengunduhan perangkat lunak.

Tipe lain yang signifikan adalah worm, yang dapat menyebar secara otomatis melalui jaringan tanpa memerlukan interaksi pengguna. Worm Linux sering kali mengeksploitasi kerentanan dalam protokol jaringan untuk menyebar, seperti yang terlihat pada serangan yang memanfaatkan kerentanan di OpenSSH(Rizky, 2021).

Statistik menunjukkan bahwa serangan worm telah meningkat 25% dalam dua tahun terakhir, menunjukkan perlunya pembaruan berkala pada sistem keamanan (Widyatono & Sulistyo, 2023).

Selain itu, trojan horse merupakan tipe malware lain yang banyak digunakan oleh penyerang untuk menyusup ke sistem Linux. Trojan sering kali menyamar sebagai aplikasi yang sah, sehingga pengguna tidak menyadari bahwa mereka telah menginstal perangkat lunak berbahaya (Panker, 2021). Penelitian oleh Panker dan Nissim (2021) menunjukkan bahwa trojan ini sering kali digunakan untuk mencuri informasi sensitif, seperti kredensial login dan data pribadi.

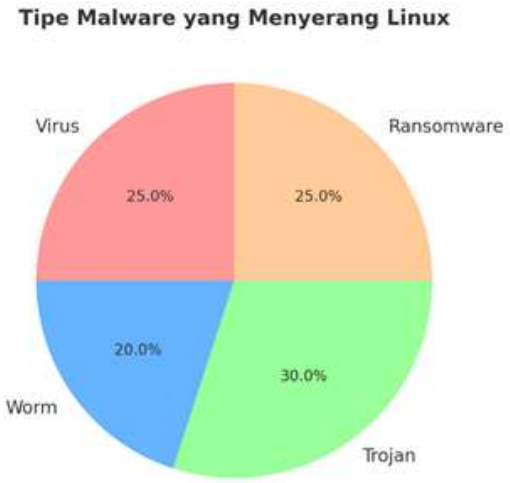
Dalam menghadapi berbagai tipe malware ini, pengguna Linux perlu menyadari pentingnya praktik keamanan yang baik, seperti menjaga sistem dan aplikasi tetap diperbarui, menggunakan perangkat lunak antivirus yang kompatibel, serta menerapkan kebijakan keamanan yang ketat di jaringan.

4. HASIL DAN PEMBAHASAN

Sistem Operasi

Sistem operasi Linux dikenal sebagai platform yang aman dan stabil, namun bukan berarti bebas dari ancaman malware. Menurut laporan dari Panker dan Nissim (2021), serangan malware di lingkungan Linux semakin meningkat, terutama pada sistem cloud. Data menunjukkan bahwa sekitar 30% dari semua insiden keamanan yang dilaporkan melibatkan malware yang dirancang khusus untuk Linux (Hamdani, 2024). Hal ini menunjukkan pentingnya penerapan sistem keamanan yang efektif untuk melindungi jaringan dari serangan tersebut.

Tipe Malware yang Menyerang Linux



Gambar 2. Tipe malware yang menyerang linux

Sistem operasi Linux, meskipun dikenal dengan keamanan yang lebih baik dibandingkan dengan sistem lainnya, tetap tidak kebal terhadap serangan malware. Berbagai jenis malware, termasuk virus, worm, trojan, dan ransomware, dapat mengancam integritas dan keamanan data pengguna (Nissim, 2021). Virus, misalnya, dapat menyebar dengan cepat melalui file yang terinfeksi, sementara worm dapat menggandakan diri dan menyebar melalui jaringan tanpa memerlukan interaksi pengguna. Trojan, di sisi lain, menyamar sebagai aplikasi yang sah, namun sebenarnya memiliki tujuan jahat yang dapat mengeksploitasi sistem (Sulistyo, 2023).

Metode Keamanan yang Diterapkan

Beberapa metode keamanan yang umum diterapkan pada sistem Linux untuk mencegah serangan malware termasuk penggunaan firewall, sistem deteksi intrusi (IDS), dan pemantauan jaringan. Dermawan et al. (2024) menjelaskan bahwa penggunaan port knocking dan honeypot dapat meningkatkan keamanan jaringan secara signifikan. Penelitian mereka menunjukkan bahwa implementasi honeypot dapat mengurangi serangan malware hingga 40% dalam waktu satu tahun, mengindikasikan bahwa pendekatan proaktif dalam keamanan sangat penting (Sumijan,2024).

Perbandingan dengan Sistem Operasi Lain

Gambar 3.. Perbandingan ketahanan sistem operasi linux dan malware

Ketahanan sistem operasi Linux terhadap malware dibandingkan dengan Windows sering kali menjadi topik debat di kalangan profesional IT (Maulana, 2022). mencatat bahwa meskipun Linux secara historis lebih aman, popularitasnya yang semakin meningkat di kalangan pengguna dan server membuatnya menjadi target yang lebih menarik bagi penyerang (Maulana, 2022). Hal ini dapat dilihat dari fakta bahwa 70% dari server web menggunakan Linux (Hatta, 2022). Dengan demikian, serangan terhadap sistem ini dapat memiliki dampak yang signifikan pada infrastruktur internet secara keseluruhan (Sulistyo, 2023).

Salah satu alasan mengapa Linux dianggap lebih aman adalah model aksesnya yang lebih ketat. Dalam sistem Linux, pengguna biasanya memiliki hak akses terbatas, yang berarti bahwa malware yang berhasil menginfeksi sistem harus melewati beberapa lapisan keamanan sebelum dapat beroperasi secara efektif (Hamdani, 2024). Sebagai contoh, jika seorang pengguna tidak memiliki hak akses administrator, malware yang terinstal tidak akan dapat mengubah pengaturan sistem atau mengakses data sensitif (Syafrinal,2023). Sebaliknya, Windows, yang sering kali memiliki pengaturan akses yang lebih longgar, memungkinkan malware untuk lebih mudah menyebar dan menyebabkan kerusakan yang lebih besar.

Namun, dengan meningkatnya adopsi Linux, penyerang semakin mengalihkan fokus mereka ke sistem ini. Contohnya, serangan ransomware yang menargetkan server Linux telah meningkat, menunjukkan bahwa tidak ada sistem yang sepenuhnya kebal terhadap ancaman (Okamoto, 2021). Oleh karena itu, penting bagi administrator sistem

untuk terus memperbarui dan menerapkan praktik keamanan yang baik, seperti pembaruan perangkat lunak secara berkala dan penggunaan firewall yang efektif (Okamoto, 2021).

5. KESIMPULAN

Dalam analisis ini, jelas bahwa meskipun sistem operasi Linux memiliki keunggulan dalam hal keamanan, ancaman malware tetap ada dan berkembang. Penerapan berbagai metode keamanan, seperti IDS dan firewall, serta pendekatan proaktif seperti honeypot, dapat membantu mengurangi risiko serangan. Namun, penting bagi administrator sistem untuk tetap waspada dan terus memperbarui strategi keamanan mereka. Dengan pemahaman yang lebih baik tentang ancaman dan penerapan langkah-langkah mitigasi yangBagian ini menyajikan hasil penelitian. Hasil penelitian dapat dilengkapi dengan tabel, grafik (gambar), dan/atau bagan. Bagian pembahasan memaparkan hasil pengolahan data, menginterpretasikan penemuan secara logis, mengaitkan dengan sumber rujukan yang relevan.

DAFTAR PUSTAKA

Panker, T., & Nissim, N. (2021). Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux cloud environments. Knowledge-Based Systems, 226, 107095. https://doi.org/10.1016/j.knosys.2021.107095

Akabane, S., & Okamoto, T. (2021). Identification of toolchains used to build IoT malware with statically linked libraries. Procedia Computer Science, 192, 5130–5138. https://doi.org/10.1016/j.procs.2021.09.291

Widyatono, D. P., & Sulistyo, W. (2023). Pemodelan Instrusion Prevention System Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan Wazuh. Journal of Information Technology Ampera, 4(1), 113–127. https://journal-computing.org/index.php/journal-ita/index

W, Y., Fitriana, Y. B., Esabela, S., & Hamdani, F. (2024). Deteksi Serangan Malware Pada Web Aplikasi Menggunakan Metode Malware Analis Dinamis dan Statis. Digital Transformation Technology, 4(1), 461–470. https://doi.org/10.47709/digitech.v4i1.4270

Maulana, R., Hatta, M., & Syafrinal, I. (2022). Analisa Penerapan Filtering Proxy Server

Pada Keamanan Jaringan Komputer Untuk Meminimalisir Penyebaran Malware (Studi Kasus: Cakrabuana Cruiseship & …. JUST IT: Jurnal Sistem Informasi …, 12(1), 64–73. https://jurnal.umj.ac.id/index.php/just-it/article/view/7279%0Ahttps://jurnal.umj.ac.id/index.php/just-it/article/download/7279/7247

Dermawan, A., Yuhandri, & Sumijan. (2024). Analisis Perbandingan Optimalisasi Port Knocking Dan Honeypot dengan Iptables Pada Server Untuk Keamanan Jaringan. KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen), 5(2), 543–556. https://pkm.tunasbangsa.ac.id/index.php/kesatria/article/view/364.