BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 1, Juni Tahun 2024
ISSN 3024-8248 (media online)
Hal 72-76

Keamanan Siber Pada Distribusi Linux: Studi Kasus Dan Solusi Efektif

Sofyan Mufti Prasetiyo[1*], Susana Familia Ulu[2], Halomoan Simatupang[3], Jevi Kerwinto Nahak[4]

[1]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: [1]dosen018009@unpam.ac.id, [2*]susanafamiliaulu@gmail.com,
[3*]halomoansimatupang0605@gmail.com, [4*]jhefrynahack24@gmail.com
(* : coresponden author : dosen01809@unpam.ac.id)

Abstrak − Keamanan siber pada distribusi Linux menjadi isu krusial dalam era digital saat ini, dengan meningkatnya kompleksitas dan frekuensi serangan yang menargetkan infrastruktur informasi. Distribusi Linux, yang dikenal dengan sifat terbuka dan fleksibelnya, menjadi sasaran yang menarik bagi penyerang yang ingin mengeksploitasi kerentanan untuk memperoleh akses tidak sah atau merusak sistem. Penelitian ini melakukan tinjauan literatur komprehensif terhadap keamanan siber pada distribusi Linux, dengan fokus pada studi kasus dan solusi efektif yang diterapkan dalam lima tahun terakhir (2019-2024). Pencarian literatur dilakukan menggunakan database Google Scholar dengan kata kunci "keamanan siber", "sistem operasi Linux", dan "studi kasus keamanan". Kriteria inklusi meliputi relevansi dengan topik, publikasi dalam bahasa Indonesia, dan metode yang jelas. Studi yang dipilih dievaluasi berdasarkan relevansi, metodologi, dan kredibilitas sumber. Hasil penelitian mengidentifikasi bahwa implementasi teknologi deteksi intrusi berbasis tanda tangan dan anomali, serta pemanfaatan pembelajaran mesin, telah menjadi pendekatan yang umum digunakan untuk meningkatkan keamanan distribusi Linux. Studi kasus juga menunjukkan berbagai teknik perlindungan, seperti firewall yang dikonfigurasi dengan baik dan teknik enkripsi, yang efektif mengurangi risiko serangan siber. Temuan ini memberikan wawasan yang berharga bagi praktisi keamanan siber dan peneliti untuk mengembangkan strategi yang lebih baik dalam melindungi infrastruktur yang menggunakan sistem operasi Linux dari ancaman siber yang terus berkembang.

Kata Kunci: Keamanan Siber; Sistem Operasi Linux; Studi Kasus Keamanan;

Abstract *− Cybersecurity in Linux distributions has become a critical issue in today's digital era, with increasing complexity and frequency of attacks targeting information infrastructures. Linux distributions, known for their open-source and flexible nature, have become attractive targets for attackers seeking to exploit vulnerabilities to gain unauthorized access or disrupt systems. This research conducts a comprehensive literature review on cybersecurity in Linux distributions, focusing on case studies and effective solutions implemented in the last five years (2019-2024). Literature search was performed using Google Scholar database with keywords "cybersecurity", "Linux operating system", and "security case studies". Inclusion criteria encompassed relevance to the topic, publication in the Indonesian language, and clear methodologies. Selected studies were evaluated based on relevance, methodology, and source credibility. The research findings identify that the implementation of signature-based and anomaly-based intrusion detection technologies, coupled with machine learning applications, has become a prevalent approach to enhancing the security of Linux distributions. Case studies also demonstrate various protection techniques, such as well-configured firewalls and encryption methods, effectively mitigating cybersecurity risks. These findings provide valuable insights for cybersecurity practitioners and researchers to develop improved strategies in safeguarding infrastructure using Linux operating systems from evolving cyber threats..*

Keywords*: Cybersecurity; Linux Operating System; Security Case Studies.*

1. PENDAHULUAN

Keamanan jaringan komputer mencakup berbagai resource apa saja yang terdapat di dalam jaringan komputer tersebut, baik itu jaringan yang bersifat network public (jaringan umum) maupun jaringan yang bersifat network private (jaringan pribadi)(Khadafi, Pratiwi, and Alfianto 2021). Kepentingan Keamanan siber telah menjadi salah satu isu utama dalam era digital saat ini, yang mempengaruhi berbagai aspek kehidupan mulai dari bisnis, pemerintahan, hingga kehidupan pribadi. Serangan siber semakin berkembang dalam kompleksitas dan kerusakan yang ditimbulkannya, mengancam infrastruktur informasi yang vital dan data sensitif pengguna. Distribusi Linux, sebagai salah satu sistem operasi open-source yang paling banyak digunakan di dunia, tidak terkecuali dari ancaman ini. Linux digunakan dalam berbagai aplikasi kritis termasuk

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 1, Juni Tahun 2024
ISSN 3024-8248 (media online)
Hal 72-76

server web, jaringan, perangkat IoT, dan komputasi awan (cloud computing), menjadikannya target yang menarik bagi penyerang.

Sifat terbuka dan fleksibel dari Linux memberikan keuntungan dalam hal kemampuan kustomisasi dan pengembangan yang cepat. Namun, hal ini juga memperkenalkan risiko keamanan yang signifikan. Kerentanan dalam distribusi Linux dapat dieksploitasi oleh penyerang untuk melakukan serangan siber yang berpotensi merusak atau merugikan organisasi atau individu yang mengandalkan sistem tersebut untuk menjalankan operasi sehari-hari mereka. Contohnya, celah keamanan dalam konfigurasi web server Linux bisa dimanfaatkan untuk mengakses data sensitif atau bahkan mengganggu layanan yang disediakan oleh server tersebut.

Dalam beberapa tahun terakhir, penelitian tentang keamanan siber pada distribusi Linux telah mengalami perkembangan pesat. Para peneliti dan praktisi keamanan siber terus mencari solusi yang efektif untuk mengidentifikasi, mencegah, dan merespons serangan yang berpotensi merusak ini. Tinjauan literatur tentang topik ini menjadi penting untuk memahami perkembangan terbaru dalam teknologi keamanan yang digunakan untuk melindungi distribusi Linux dari ancaman siber yang semakin kompleks.

2. METODE PENELITIAN

2.1 Tujuan Tinjauan

Tujuan tinjauan literatur ini adalah untuk mengidentifikasi dan menganalisis penelitian yang telah dilakukan tentang Keamanan Siber pada Distribusi Linux: Studi Kasus dan Solusi Efektif. Tinjauan ini mencakup literatur yang dipublikasikan dalam lima tahun terakhir dan berfokus pada studi kuantitatif dan kualitatif.

2.2 Pencarian Literatur

Pencarian literatur dilakukan menggunakan database Google Scholar.Kata kunci yang digunakan termasuk "keamanan siber", "sistem operasi linux", dan "studi kasus keamanan". Kriteria inklusi mencakup studi yang dipublikasikan dalam lima tahun terakhir, relevan dengan topik, dan tersedia dalam bahasa Inggris. Studi yang tidak memiliki abstrak yang relevan atau metode yang jelas dikeluarkan.

2.3 Evaluasi Literatur

Literatur dievaluasi berdasarkan relevansi, validitas metodologi, dan kredibilitas sumber. Seleksi awal dilakukan berdasarkan judul dan abstrak, diikuti oleh seleksi lanjutan berdasarkan teks lengkap. Setiap studi yang dipilih dievaluasi menggunakan kerangka kerja kritis untuk memastikan kualitas dan relevansinya.

2.4 Analisis dan Sintesis

Analisis tematik dilakukan untuk mengidentifikasi tema utama yang muncul dari literatur, seperti praktik melindungi. Literatur dikelompokkan berdasarkan tema-tema ini dan dibandingkan untuk mengidentifikasi kesamaan dan perbedaan dalam temuan.

2.5 Penyajian Hasil

Hasil tinjauan literatur menunjukkan bahwa adanya kelemahan dalam sistem dalam mendeteksi serangan jaringan. Web server memerlukan sistem keamanan yang mampu melindungi dari berbagai jenis serangan dan upaya penyusupan atau pemindaian oleh pihak ketiga. Tahap desain melibatkan penerapan rancangan dari berbagai elemen yang dibutuhkan pada tahap sebelumnya sebagai bagian dari konfigurasi aplikasi atau sistem (Soesanto et al. 2023).

Temuan utama dalam penelitian ini yaitu:

1. Sistem Detteksi Intrusi (IDS)

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 1, Juni Tahun 2024
ISSN 3024-8248 (media online)
Hal 72-76

a. Sistem IDS berbasis tanda tangan(signature-based IDS)seperti Snort seringkali tidak mampu mendeteksi serangan baru(Zero-day attacks) karena tergantung pada basis data tanda tangan yang sudah ada (Khraisat et al. 2019)

b. Pendekatan berbasis anomaly (anomaly-based IDS) lebih efektif salam mendeteksi aktivitas mencurigakan yang tidak terdefinisikan dalam basis data tanda tangan. Namun, mereka memiliki tingkat false positive yang tinggi (Ilzam et al. 2024)

2. Metode Pembelajaran Mesin dan Deep Learning

a. Teknik pembelajaran mesin, termasuk SVM dengan embedding fitur Naive Bayes, telah menunjukkan peningkatan dalam deteksi intrusi dengan menggabungkan berbagai fitur keamanan

b. Deep learning dan jaringan saraf konvolusional juga digunakan untuk mengembangkan sistem IDS yang lebih adaptif dan mampu belajar dari data lalu lintas jaringan secara real-time(Ilzam et al. 2024)

3. Studi Kasus Distribusi Linux

a. Studi kasus pada distribusi Linux seperti Kali Linux menunjukkan bahwa penggunaan alat keamanan seperti Suricata dan firewall yang dikonfigurasi dengan baik dapat meningkatkan pertahanan terhadap serangan siber.

b. Implementasi IDS pada sistem operasi Linux membantu dalam mengidentifikasi dan mengatasi berbagai jenis serangan yang menargetkan server web dan jaringan (Khadafi, Pratiwi, and Alfianto 2021)

4. Dalam jurnalnya , Marzuki Hasibuan dan Andi Marwan Elhani melakukan Penetration testing sistem jarigan computer menggunakan kali linux Untk mengetahui kerentanan server dengan metode black box

a. Dari hasil laporan information gathering didapatkan beberapa port yang terbuka dan ditemukan informasi DNS (Domain Name Server) yang digunakan web server www.divakaraoke.co.id

b. Dari hasil laporan jenis kerentanan ditemukan 3 jenis kerentanan.

1) X-Frame-Options Header Not Set

2) Cross-Domain JavaScript Source File Inclusion,

3) X-Content-Type-Options Header Missing.

c. Dari hasil laporan dampak dan resiko webserver www.divakaraoke.co.id rentan terhadap serangan clickjacking dan serangan sniffing MIME

3. ANALISA DAN PEMBAHASAN

3.1 Dasar-Dasar Teori

a. IDS

Intrusion Detection System (IDS) adalah teknik yang digunakan oleh admin jaringan untuk mengamankan akses jaringan komputer dari penyusup(Khadafi, Pratiwi, and Alfianto 2021). IDS mendeteksi aktivitas mencurigakan di jaringan dengan empat tahapan utama:

1. Knowledge-based: Mengenali penyusupan dengan membandingkan paket data dengan database rule IDS yang berisi tanda-tanda paket serangan.

2. Behavior-based (anomaly): Mendeteksi penyusupan dengan mengamati kejanggalan atau penyimpangan dari kondisi normal sistem.

3. Passive IDS: Bertindak sebagai pendeteksi yang menghasilkan alarm jika terdeteksi gangguan.

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 1, Juni Tahun 2024
ISSN 3024-8248 (media online)
Hal 72-76

4. Reactive IDS: Bertindak sebagai pendeteksi, pemberi peringatan, dan mengambil tindakan pemblokiran terhadap serangan.

IDS memiliki lima jenis utama berdasarkan kemampuannya:

1. Network Intrusion Detection System (NIDS)*: Mengawasi lalu lintas jaringan data dengan menggunakan peranti jaringan yang dilengkapi dengan Network Interface Card (NIC).
2. Host-based Intrusion Detection System (HIDS)
3. Protocol-based Intrusion Detection System (PIDS)
4. Application Protocol-based Intrusion Detection System (APIDS)
5. Hybrid-based Intrusion Detection System (HIDS)

3.2 Ringkasan Temuan Utama

Penelitian ini mengidentifikasi bahwa ada dua pendekatan utama dalam sistem deteksi intrusi (IDS) yang digunakan dalam distribusi Linux: IDS berbasis tanda tangan (signature-based IDS) dan IDS berbasis anomali (anomaly-based IDS). IDS berbasis tanda tangan, seperti Snort, ditemukan kurang efektif dalam mendeteksi serangan zero-day karena ketergantungannya pada basis data tanda tangan yang ada. Sebaliknya, IDS berbasis anomali lebih efektif dalam mendeteksi aktivitas mencurigakan yang tidak terdefinisikan dalam basis data tanda tangan, meskipun memiliki tingkat false positive yang tinggi. Selain itu, metode pembelajaran mesin dan deep learning menunjukkan potensi besar dalam meningkatkan deteksi intrusi dengan menggabungkan berbagai fitur keamanan.

3.3 Analisis Temuan

DS berbasis tanda tangan, seperti yang diuraikan oleh Khraisat et al. (2019), memiliki keunggulan dalam mendeteksi serangan yang sudah dikenal namun gagal dalam menghadapi serangan zero-day. Hal ini disebabkan oleh ketergantungan pada basis data tanda tangan yang hanya mencakup serangan yang sudah diketahui. Keberhasilan IDS berbasis tanda tangan sangat bergantung pada kecepatan pembaruan dan akurasi basis data tanda tangan.

Di sisi lain, IDS berbasis anomali memiliki pendekatan yang berbeda. Sistem ini memantau lalu lintas jaringan dan mencari pola yang tidak biasa atau anomali yang dapat menunjukkan adanya serangan. Pendekatan ini lebih efektif dalam mendeteksi serangan zero-day karena tidak bergantung pada basis data tanda tangan yang ada. Namun, kelemahan utama dari IDS berbasis anomali adalah tingginya tingkat false positive, di mana aktivitas normal terkadang salah diidentifikasi sebagai serangan (Ilzam et al. 2024). Hal ini dapat mengakibatkan kewaspadaan berlebihan dan penggunaan sumber daya yang tidak efisien untuk menindaklanjuti peringatan yang salah.

Metode pembelajaran mesin, seperti SVM dengan embedding fitur Naive Bayes, telah menunjukkan peningkatan dalam deteksi intrusi dengan menggabungkan berbagai fitur keamanan (Ilzam et al. 2024). Pendekatan ini memanfaatkan kemampuan SVM untuk melakukan klasifikasi dengan akurasi tinggi, sementara embedding fitur Naive Bayes membantu dalam mengidentifikasi pola yang lebih kompleks dalam data. Teknik ini memungkinkan sistem untuk mendeteksi serangan dengan lebih akurat dan responsif terhadap perubahan dalam pola serangan. Teknik deep learning, termasuk jaringan saraf konvolusional, juga digunakan untuk mengembangkan sistem IDS yang lebih adaptif dan mampu belajar dari data lalu lintas jaringan secara real-time Deep learning menawarkan keunggulan dalam hal kemampuan untuk menangani volume data yang besar dan kompleks, serta mampu mengenali pola yang lebih halus yang mungkin terlewatkan oleh metode deteksi tradisional. Jaringan saraf konvolusional khususnya, dikenal efektif dalam pemrosesan data spasial dan temporal, yang relevan dalam konteks analisis lalu lintas jaringan.

Temuan ini relevan dalam konteks keamanan siber pada distribusi Linux karena menunjukkan bahwa kombinasi metode IDS dan pembelajaran mesin dapat meningkatkan deteksi intrusi. Praktisi keamanan siber dapat menerapkan metode ini untuk melindungi sistem dari serangan yang semakin canggih. Misalnya, kombinasi IDS berbasis tanda tangan dan IDS berbasis anomali

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 1, Juni Tahun 2024
ISSN 3024-8248 (media online)
Hal 72-76

dapat memberikan perlindungan yang lebih komprehensif, di mana kelemahan satu pendekatan dapat diimbangi oleh kekuatan pendekatan lainnya.

Studi kasus pada distribusi Linux, seperti penggunaan Kali Linux dengan alat keamanan seperti Suricata dan konfigurasi firewall yang baik, menunjukkan bahwa langkah-langkah ini dapat meningkatkan pertahanan terhadap serangan siber. Kali Linux, dengan alat keamanan yang kuat dan kemampuan untuk disesuaikan, memberikan platform yang ideal untuk menguji dan mengimplementasikan berbagai teknik deteksi intrusi. Suricata, sebagai IDS yang canggih, mampu menganalisis lalu lintas jaringan dengan detail dan mendeteksi serangan dalam waktu nyata.

Implementasi IDS pada sistem operasi Linux membantu dalam mengidentifikasi dan mengatasi berbagai jenis serangan yang menargetkan server web dan jaringan. Hal ini menjadi semakin penting dalam lingkungan yang semakin terhubung dan rentan terhadap serangan siber yang kompleks. Misalnya, IDS yang diterapkan pada server web dapat memantau lalu lintas masuk dan keluar, mendeteksi upaya penyusupan, dan memberikan peringatan dini tentang potensi serangan.

4. KESIMPULAN

Tinjauan literatur ini menunjukkan bahwa kombinasi berbagai metode IDS dan pembelajaran mesin dapat meningkatkan keamanan siber pada distribusi Linux. Implementasi solusi ini dapat membantu melindungi sistem dari serangan yang semakin canggih dan beragam, memberikan kontribusi signifikan terhadap praktik keamanan siber saat ini. Penggunaan teknik IDS berbasis tanda tangan dan anomali, bersama dengan metode pembelajaran mesin yang canggih, dapat memberikan perlindungan yang lebih komprehensif dan adaptif terhadap ancaman siber.

Dengan mengakui keterbatasan yang ada dan terus mengeksplorasi solusi inovatif, komunitas keamanan siber dapat terus meningkatkan kemampuan mereka dalam mendeteksi dan mencegah serangan, melindungi infrastruktur kritis, dan menjaga integritas data dalam lingkungan yang semakin terhubung dan kompleks.

Dengan struktur dan detail ini, bagian pembahasan Anda akan lebih lengkap, mendalam, dan memberikan wawasan yang berharga bagi pembaca. Ini juga akan memastikan bahwa temuan dan rekomendasi Anda didukung oleh analisis yang kuat dan relevan.

REFERENCES

Ilzam, Nur, Che Mat, Norziana Jamil, Yunus Yusoff, and Laiha Mat Kiah. 2024. “Review Article A Systematic Literature Review on Advanced Persistent Threat Behaviors and Its Detection Strategy.” : 1–18.

Khadafi, Shah, Yuni Dian Pratiwi, and Enggar Alfianto. 2021. “KEAMANAN FTP SERVER BERBASISKAN IDS DAN IPS.” 6(1): 11–24.

Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. 2019. “Survey of Intrusion Detection Systems : Techniques , Datasets and Challenges.”

Soesanto, Edy, Achmad Romadhon, Bima Dwi Mardika, and Moch Fahmi Setiawan. 2023. “Analisis Dan Peningkatan Keamanan Cyber : Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File.” 1(2): 172–91.