e-XXXX-XXXX

Original Article

Pengujian Keamanan Server Linux terhadap Serangan Port Scanning dan Exploitation

Muh. Dirga Asmadi[1], Syahril Zaldi[2] ✉, Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: muhdirgaasmadi.241031104@mahasiswa.ith,ac.id[1],
syahrilzaldi.241031096@mahasiswa.ith.ac.id[2] ✉ , rakhmadi.rahman@ith.ac.id[3]

Abstrak:

Keamanan server merupakan aspek fundamental dalam penyelenggaraan layanan teknologi informasi, terutama pada sistem operasi Linux yang banyak digunakan sebagai server karena sifatnya yang stabil, fleksibel, dan bersifat open source. Tingginya tingkat adopsi Linux sebagai server juga menjadikannya target utama berbagai bentuk serangan siber. Salah satu metode serangan yang paling umum adalah port scanning yang bertujuan untuk mengidentifikasi port terbuka dan layanan aktif, yang selanjutnya dapat dimanfaatkan untuk melakukan exploitation terhadap celah keamanan yang ada. Penelitian ini bertujuan untuk menguji tingkat keamanan sebuah server Linux terhadap serangan port scanning dan exploitation serta menganalisis potensi kerentanan yang dapat dimanfaatkan oleh penyerang. Metode penelitian yang digunakan adalah pendekatan eksperimental dengan melakukan simulasi serangan menggunakan tools keamanan, yaitu Nmap untuk port scanning dan Metasploit Framework untuk exploitation. Lingkungan pengujian dirancang dalam jaringan lokal dengan satu mesin server Linux sebagai target dan satu mesin penyerang. Hasil pengujian menunjukkan bahwa port scanning mampu mengungkap informasi penting terkait port terbuka, layanan yang berjalan, serta versi layanan yang digunakan. Informasi ini dapat menjadi dasar bagi penyerang untuk menentukan teknik exploitation yang sesuai. Selain itu, hasil exploitation menunjukkan bahwa server Linux yang tidak menerapkan pembaruan sistem secara berkala, konfigurasi firewall yang ketat, dan pengamanan layanan dasar memiliki tingkat kerentanan yang lebih tinggi. Penelitian ini menegaskan pentingnya penerapan hardening server Linux sebagai langkah preventif dalam menghadapi ancaman siber.

Keywords: Keamanan Server, Linux, Port Scanning, Exploitation, Cyber Security.

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026

Pendahuluan

Perkembangan teknologi informasi yang pesat telah mendorong peningkatan penggunaan server dalam berbagai sektor, mulai dari pendidikan, pemerintahan, hingga industri. Server berperan sebagai pusat pengolahan, penyimpanan, dan distribusi data, sehingga memiliki nilai strategis yang tinggi. Oleh karena itu, aspek keamanan server menjadi perhatian utama dalam pengelolaan infrastruktur teknologi informasi.

Sistem operasi Linux merupakan salah satu platform yang paling banyak digunakan sebagai server karena keunggulannya dalam hal stabilitas, performa, dan sifat open source. Meskipun Linux dikenal memiliki tingkat keamanan yang baik, sistem ini tetap berpotensi mengalami serangan siber apabila tidak dikelola dan dikonfigurasi dengan baik. Banyak kasus pelanggaran keamanan terjadi bukan karena kelemahan sistem operasi itu sendiri, melainkan akibat kesalahan konfigurasi dan kelalaian dalam penerapan kebijakan keamanan. Dalam siklus serangan siber, port scanning merupakan tahap awal yang krusial. Teknik ini digunakan untuk mengidentifikasi port terbuka dan layanan aktif pada sebuah server. Informasi yang diperoleh dari port scanning sering kali dimanfaatkan oleh penyerang untuk melanjutkan serangan ke tahap berikutnya, yaitu exploitation. Exploitation dilakukan dengan memanfaatkan celah keamanan pada layanan atau aplikasi yang berjalan di server untuk memperoleh akses ilegal.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada pengujian keamanan server Linux terhadap serangan port scanning dan exploitation. Rumusan masalah dalam penelitian ini adalah bagaimana tingkat keamanan server Linux terhadap kedua jenis serangan tersebut serta kerentanan apa saja yang berpotensi dieksploitasi. Penelitian ini bertujuan untuk memberikan gambaran nyata mengenai risiko keamanan server Linux dan memberikan rekomendasi pengamanan yang dapat diterapkan. Penelitian ini diharapkan dapat meningkatkan kesadaran akan pentingnya keamanan server dalam bidang Cyber Security. Selain itu, meningkatnya kompleksitas serangan siber di era digital menunjukkan bahwa ancaman terhadap server tidak lagi bersifat sederhana atau acak, melainkan terstruktur dan terencana dengan baik. Penyerang memanfaatkan berbagai teknik otomatisasi dan eksploitasi berbasis tool untuk menemukan celah keamanan dalam waktu singkat. Kondisi ini menuntut administrator sistem dan praktisi teknologi informasi untuk tidak hanya memahami konsep dasar keamanan, tetapi juga mampu melakukan pengujian keamanan secara aktif guna mengidentifikasi kelemahan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Pengujian keamanan server melalui simulasi serangan seperti port scanning dan exploitation merupakan bagian dari pendekatan penetration testing yang bersifat preventif. Pendekatan ini memungkinkan pengelola sistem untuk melihat server dari sudut pandang penyerang, sehingga dapat memahami pola serangan yang mungkin terjadi. Dengan demikian, hasil pengujian tidak hanya berfungsi sebagai evaluasi teknis, tetapi juga sebagai dasar dalam penyusunan kebijakan keamanan dan peningkatan kapasitas sumber daya manusia di bidang Cyber Security. Dalam konteks akademik, penelitian mengenai pengujian keamanan server Linux memiliki relevansi yang tinggi karena mengintegrasikan teori dan praktik keamanan informasi. Mahasiswa tidak hanya mempelajari konsep keamanan secara konseptual, tetapi juga memahami implementasi nyata di lapangan melalui penggunaan tools dan metode yang umum digunakan dalam industri. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi baik secara akademis maupun praktis dalam pengembangan kompetensi di bidang Riset Teknologi Informasi dan Cyber Security.

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026

Tinjauan Pustaka

Konsep Keamanan Informasi

Keamanan informasi merupakan disiplin ilmu yang berfokus pada upaya perlindungan terhadap aset informasi dari berbagai ancaman, baik yang bersifat internal maupun eksternal. Tujuan utama keamanan informasi adalah menjaga kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) informasi yang dikenal sebagai konsep CIA Triad. Ketiga aspek ini menjadi landasan dalam perancangan dan implementasi sistem keamanan pada infrastruktur teknologi informasi, termasuk server.

Dalam konteks server, keamanan informasi tidak hanya berkaitan dengan perlindungan data yang disimpan, tetapi juga mencakup pengamanan layanan, sistem operasi, serta jaringan yang terhubung. Kegagalan dalam menjaga salah satu aspek CIA Triad dapat berdampak pada kerugian finansial, reputasi organisasi, hingga gangguan operasional. Oleh karena itu, keamanan server harus dipandang sebagai kebutuhan strategis dan berkelanjutan.

Linux merupakan sistem operasi berbasis open source yang banyak digunakan sebagai server di berbagai sektor. Keunggulan Linux terletak pada stabilitas, fleksibilitas, serta dukungan komunitas yang luas. Selain itu, model pengembangan open source memungkinkan proses audit kode secara terbuka, sehingga potensi celah keamanan dapat ditemukan dan diperbaiki dengan cepat.

Meskipun demikian, keamanan Linux sangat bergantung pada konfigurasi dan pengelolaannya. Linux menyediakan berbagai mekanisme keamanan bawaan, seperti manajemen hak akses berbasis user dan group, firewall (iptables atau nftables), serta sistem kontrol akses seperti SELinux dan AppArmor. Namun, tanpa konfigurasi yang tepat, mekanisme tersebut tidak akan berfungsi secara optimal dan justru dapat menimbulkan celah keamanan baru.

Konsep Port dan Layanan Jaringan

Port merupakan endpoint logis yang digunakan oleh sistem operasi untuk mengatur dan mengidentifikasi komunikasi data antara perangkat dalam suatu jaringan. Port bekerja bersama alamat IP untuk memastikan bahwa data yang dikirimkan melalui jaringan dapat diteruskan ke layanan atau aplikasi yang tepat. Setiap port diidentifikasi dengan nomor tertentu dalam rentang 0 hingga 65535, yang secara umum dibagi menjadi well-known ports, registered ports, dan dynamic/private ports. Well-known ports biasanya digunakan oleh layanan standar, seperti port 22 untuk Secure Shell (SSH), port 80 untuk Hypertext Transfer Protocol (HTTP), dan port 443 untuk Hypertext Transfer Protocol Secure (HTTPS).

Dalam implementasinya, layanan jaringan seperti web server, mail server, file server, dan database server bergantung pada port tertentu untuk menerima dan mengirimkan data. Ketika sebuah layanan aktif pada suatu port, sistem operasi akan membuka port tersebut dan menunggu permintaan dari klien. Status port dapat diklasifikasikan ke dalam beberapa kondisi, yaitu terbuka (open), tertutup (closed), atau difilter (filtered). Port dengan status terbuka menandakan bahwa terdapat layanan yang aktif dan dapat diakses, port tertutup menunjukkan tidak adanya layanan yang berjalan, sedangkan port difilter biasanya dilindungi oleh mekanisme keamanan seperti firewall sehingga tidak dapat diakses secara langsung.

Keberadaan port terbuka pada sebuah server merupakan kebutuhan fungsional

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026

agar layanan dapat berjalan dan diakses oleh pengguna yang sah. Namun demikian, port terbuka juga menjadi salah satu titik utama yang dieksploitasi dalam serangan siber. Setiap port terbuka berpotensi menjadi pintu masuk bagi penyerang untuk melakukan eksploitasi, terutama jika layanan yang berjalan memiliki kerentanan atau dikonfigurasi secara tidak aman. Oleh karena itu, jumlah dan jenis port yang terbuka pada sebuah server secara langsung memengaruhi tingkat risiko keamanan sistem tersebut.

Dalam konteks keamanan jaringan, konsep permukaan serangan (attack surface) menjadi sangat penting. Permukaan serangan merujuk pada seluruh titik yang dapat diakses atau diserang oleh pihak eksternal, termasuk port terbuka dan layanan yang berjalan di atasnya. Semakin banyak port dan layanan yang aktif, semakin luas pula permukaan serangan yang dimiliki oleh server. Kondisi ini meningkatkan peluang bagi penyerang untuk menemukan celah keamanan melalui teknik reconnaissance dan port scanning.

Prinsip dasar keamanan jaringan menganjurkan penerapan konsep least privilege dan minimal service exposure, yaitu hanya mengaktifkan port dan layanan yang benar-benar dibutuhkan untuk operasional sistem. Layanan yang tidak digunakan sebaiknya dinonaktifkan, dan port yang tidak diperlukan harus ditutup atau dibatasi aksesnya menggunakan firewall. Selain itu, pengamanan tambahan seperti pembatasan alamat IP, penggunaan autentikasi yang kuat, serta enkripsi komunikasi juga diperlukan untuk meminimalkan risiko serangan terhadap port yang harus tetap terbuka.

Dengan demikian, pemahaman yang mendalam mengenai konsep port dan layanan jaringan menjadi aspek fundamental dalam pengelolaan keamanan server. Pengelola sistem perlu memahami tidak hanya fungsi port dan layanan, tetapi juga implikasi keamanannya. Dalam penelitian ini, konsep port dan layanan jaringan menjadi dasar utama dalam menganalisis hasil port scanning dan menentukan potensi risiko exploitation pada server Linux yang diuji.

Port Scanning Sebagai Tahap Reconnaissance

Port scanning merupakan teknik yang digunakan untuk mengidentifikasi port terbuka dan layanan aktif pada sebuah sistem. Dalam siklus serangan siber, port scanning termasuk dalam tahap reconnaissance atau information gathering. Teknik ini memungkinkan penyerang untuk memperoleh gambaran awal mengenai sistem target sebelum melancarkan serangan lanjutan.

Dari sisi keamanan defensif, port scanning juga digunakan secara legal dalam audit keamanan dan penetration testing. Tools seperti Nmap mampu melakukan berbagai jenis pemindaian, mulai dari pemindaian sederhana hingga deteksi sistem operasi dan versi layanan. Informasi yang dihasilkan dari port scanning sangat berguna dalam proses evaluasi keamanan server.

Exploitation dan Kerentanan Sistem

Exploitation adalah proses pemanfaatan kerentanan pada sistem, aplikasi, atau layanan untuk memperoleh akses tidak sah. Kerentanan dapat muncul akibat kesalahan pemrograman, penggunaan perangkat lunak usang, atau konfigurasi sistem yang tidak aman. Dalam banyak kasus, exploitation dilakukan setelah penyerang berhasil mengidentifikasi target melalui port scanning.

Selain faktor teknis seperti kesalahan pemrograman dan penggunaan perangkat lunak usang, kerentanan sistem juga sering muncul akibat kelemahan dalam kebijakan

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026

keamanan dan praktik administrasi sistem. Penggunaan kredensial default, lemahnya mekanisme autentikasi, serta kurangnya pembatasan hak akses dapat memperbesar peluang keberhasilan exploitation. Dalam banyak kasus, penyerang tidak perlu mengeksploitasi celah yang kompleks, melainkan cukup memanfaatkan konfigurasi yang tidak aman untuk memperoleh akses ke sistem target.

Exploitation tidak hanya berdampak pada aspek kerahasiaan data, tetapi juga dapat mengancam keutuhan dan ketersediaan sistem. Serangan yang berhasil dapat memungkinkan penyerang untuk memodifikasi data, menyisipkan malware, atau bahkan melumpuhkan layanan melalui serangan lanjutan. Pada server Linux, exploitation terhadap layanan tertentu dapat berkembang menjadi eskalasi hak akses (privilege escalation), di mana penyerang yang awalnya memiliki akses terbatas dapat memperoleh hak administratif penuh terhadap sistem.

Dalam konteks pengujian keamanan, exploitation yang dilakukan secara terkontrol berperan penting sebagai alat evaluasi efektivitas mekanisme pertahanan sistem. Hasil dari pengujian ini memberikan gambaran nyata mengenai tingkat risiko yang dihadapi server serta membantu administrator dalam menentukan prioritas mitigasi. Dengan memahami pola dan dampak exploitation, pengelola sistem dapat merancang strategi pengamanan yang lebih komprehensif, termasuk penerapan patch management, hardening sistem, dan peningkatan kesadaran keamanan bagi pengguna dan administrator.

Metode

Penelitian ini menggunakan metode eksperimental dengan pendekatan simulasi serangan. Lingkungan pengujian terdiri dari satu server Linux sebagai target dan satu mesin penyerang dalam jaringan lokal. Sistem operasi server yang digunakan adalah Linux Server dengan layanan dasar seperti SSH dan web server.

Tahapan penelitian meliputi persiapan lingkungan, pengujian port scanning, pengujian exploitation, serta analisis hasil. Port scanning dilakukan menggunakan Nmap untuk mengidentifikasi port terbuka dan layanan aktif. Selanjutnya, exploitation dilakukan menggunakan Metasploit Framework terhadap layanan yang teridentifikasi memiliki potensi kerentanan. Data yang dikumpulkan berupa hasil pemindaian port, daftar layanan aktif, serta status keberhasilan atau kegagalan exploitation. Data tersebut dianalisis untuk menilai tingkat keamanan server Linux dan mengidentifikasi faktor-faktor yang memengaruhi kerentanan sistem.

Hasil dan Pembahasan

Hasil Pengujian Port Scanning

Pengujian port scanning dilakukan menggunakan tool Nmap dengan beberapa parameter pemindaian, seperti TCP SYN scan, service version detection, dan operating system detection. Pemindaian dilakukan terhadap alamat IP server Linux yang telah disiapkan dalam jaringan lokal. Hasil pengujian menunjukkan bahwa terdapat beberapa port dalam status terbuka (open) yang menjalankan layanan penting, antara lain port 22 (SSH), port 80 (HTTP), dan port 443 (HTTPS).

Informasi yang diperoleh dari port scanning tidak hanya mencakup nomor port dan jenis layanan, tetapi juga versi layanan yang digunakan. Deteksi versi layanan ini sangat penting karena banyak kerentanan keamanan diketahui berasal dari penggunaan versi perangkat lunak yang sudah usang atau belum diperbarui. Dari hasil pemindaian, ditemukan bahwa beberapa layanan masih menggunakan versi default yang berpotensi

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026

memiliki celah keamanan.

Analisis Risiko Hasil Port Scanning

Setiap port terbuka memiliki tingkat risiko yang berbeda-beda. Port 22 (SSH), misalnya, merupakan layanan penting untuk administrasi server, namun juga sering menjadi target serangan brute force. Tanpa penerapan autentikasi yang kuat dan pembatasan akses, layanan ini dapat dimanfaatkan oleh penyerang untuk mendapatkan akses awal ke sistem.

Port 80 dan 443 yang menjalankan layanan web juga memiliki potensi risiko apabila aplikasi web yang berjalan tidak diamankan dengan baik. Kerentanan seperti misconfiguration, penggunaan library lama, dan kesalahan pengaturan hak akses dapat dimanfaatkan untuk melakukan serangan lanjutan. Oleh karena itu, hasil port scanning harus dianalisis secara menyeluruh untuk menentukan prioritas pengamanan.

Hasil Pengujian Exploitation

Tahap exploitation dilakukan dengan menggunakan Metasploit Framework terhadap layanan yang teridentifikasi memiliki potensi kerentanan. Pengujian dilakukan dalam batasan etis dan hanya bertujuan untuk mengetahui sejauh mana sistem dapat dieksploitasi. Beberapa modul exploit yang relevan diuji berdasarkan versi layanan yang terdeteksi pada tahap port scanning. Hasil pengujian menunjukkan bahwa exploitation lebih mudah dilakukan pada sistem yang tidak menerapkan pembaruan keamanan secara rutin. Pada skenario tertentu, exploit berhasil dijalankan hingga tahap memperoleh akses terbatas ke sistem. Hal ini menunjukkan bahwa kombinasi antara informasi hasil port scanning dan kelemahan konfigurasi sistem dapat meningkatkan risiko serangan yang lebih serius.

Pembahasan Keamanan dan Dampak Serangan

Temuan dalam penelitian ini menunjukkan bahwa port scanning merupakan ancaman awal yang sangat signifikan karena memberikan gambaran lengkap mengenai permukaan serangan (attack surface) sebuah server. Informasi ini memungkinkan penyerang untuk merancang strategi serangan yang lebih terarah dan efisien.

Serangan exploitation yang berhasil dapat berdampak besar terhadap keamanan sistem, mulai dari kebocoran data, gangguan layanan, hingga pengambilalihan sistem secara penuh. Dalam konteks server Linux, dampak ini dapat diminimalkan dengan penerapan prinsip keamanan berlapis (defense in depth), yang mencakup pengamanan jaringan, sistem operasi, dan aplikasi.

Strategi Mitigasi dan Hardening Server Linux

Berdasarkan hasil pengujian, beberapa strategi mitigasi yang direkomendasikan antara lain penerapan firewall untuk membatasi akses port, penggunaan autentikasi berbasis kunci pada layanan SSH, serta pembaruan sistem dan layanan secara berkala. Selain itu, penerapan intrusion detection system (IDS) dan monitoring log secara rutin dapat membantu mendeteksi aktivitas mencurigakan sejak dini. Hardening server Linux juga mencakup penghapusan layanan yang tidak diperlukan, penerapan prinsip least privilege, serta penggunaan tools keamanan tambahan seperti Fail2Ban dan SELinux. Dengan penerapan langkah-langkah tersebut, risiko serangan port scanning dan exploitation dapat dikurangi secara signifikan.

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026

Kesimpulan

Berdasarkan hasil pengujian dan pembahasan, dapat disimpulkan bahwa server Linux masih memiliki potensi kerentanan terhadap serangan port scanning dan exploitation apabila tidak dikelola dengan baik. Port scanning mampu mengungkap informasi penting terkait layanan yang berjalan, yang selanjutnya dapat dimanfaatkan untuk melakukan exploitation. Penelitian ini merekomendasikan penerapan hardening server Linux, seperti pembaruan sistem secara berkala, penggunaan firewall, pembatasan akses port, serta monitoring keamanan secara berkelanjutan. Dengan penerapan langkah-langkah tersebut, tingkat keamanan server Linux dapat ditingkatkan dan risiko serangan siber dapat diminimalkan.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, disarankan agar administrator server Linux menerapkan pembaruan sistem dan layanan secara berkala guna meminimalkan potensi kerentanan yang dapat dieksploitasi oleh penyerang. Selain itu, konfigurasi firewall yang ketat perlu diterapkan untuk membatasi akses ke port dan layanan yang tidak diperlukan, sehingga dapat mengurangi risiko serangan port scanning dan exploitation. Pengamanan layanan dasar seperti SSH juga perlu ditingkatkan melalui penerapan autentikasi yang lebih kuat, pembatasan akses berbasis alamat IP, serta penggunaan mekanisme keamanan tambahan. Selanjutnya, disarankan untuk melakukan pengujian keamanan secara rutin menggunakan tools seperti Nmap dan Metasploit Framework sebagai langkah evaluasi terhadap tingkat keamanan server.

Untuk penelitian selanjutnya, disarankan agar cakupan pengujian diperluas dengan melibatkan berbagai jenis sistem operasi server, skenario jaringan yang lebih kompleks, serta penggunaan metode pengamanan tambahan, sehingga hasil penelitian dapat memberikan gambaran yang lebih komprehensif terkait keamanan server terhadap ancaman siber.

Daftar Pustaka

Behl, A., & Behl, K. (2020). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

ENISA. (2021). Threat landscape report. European Union Agency for Cybersecurity.

Kaur, G., & Singh, A. (2020). Network security threats and attacks. International Journal of Computer Applications, 176(23), 1–6.

Nmap Project. (2022). Nmap network scanning. Insecure.Org.

OWASP. (2021). OWASP top 10 web application security risks. OWASP Foundation.

Scarfone, K., & Mell, P. (2020). Guide to intrusion detection and prevention systems. NIST.

Stallings, W. (2020). Network security essentials: Applications and standards. Pearson.

Vacca, J. R. (2021). Computer and information security handbook. Elsevier.

Zhang, Y., & Chen, X. (2022). Vulnerability exploitation analysis in Linux servers. Journal of Cyber Security Technology, 6(3), 201–215.

Received: November 10, 2025 – Revised: November 25, 2025 - Accepted: Desember 14, 2025 - Published online: January 8, 2026