Jurnal Tera
Volume 5, Issue 2, September 2025
Page 59-68

E-ISSN : 2776-9666
P-ISSN : 2776-1789

IMPLEMENTASI SISTEM KEAMANAN DATA BERBASIS KALI LINUX UNTUK MENGHADAPI SERANGAN SIBER

Tamsir Ariyadi[1], Dastin[2], Fitriani Ibrahim[3], M. Ilham Septariansyah[4]
[1,2,3,4)] Universitas Bina Darma, Palembang

Corresponding author
E-mail: tamsirariyadi@binadarma.ac.id, tegerdastin@gmail.com, ibrahimfitri896@gmail.com, ilham123hafiz@gmail.com

Diterima : 24-12-2025
Direvisi : 13-01-2026
Dipublikasi : 27-01-2026

Kata Kunci: Keamanan data, Kali Linux, Serangan Siber, analisis kerentanan, keamanan sistem informasi.

Abstrak: Penelitian ini dilakukan sebagai respons terhadap meningkatnya intensitas dan kompleksitas serangan siber yang berpotensi mengganggu integritas, kerahasiaan, dan ketersediaan data pada berbagai sistem informasi modern. Institusi maupun organisasi yang semakin bergantung pada data digital membutuhkan mekanisme perlindungan yang tidak hanya reaktif tetapi juga proaktif. Oleh karena itu, penelitian ini mengimplementasikan sistem keamanan data berbasis Kali Linux sebagai solusi yang komprehensif karena distribusi ini menyediakan berbagai perangkat keamanan seperti Nmap, OpenVAS, dan Snort yang dapat digunakan untuk mendeteksi, menganalisis, dan mencegah serangan siber. Tujuan utama penelitian ini adalah merancang sistem keamanan yang mampu meningkatkan ketahanan jaringan melalui penerapan teknik pemindaian kerentanan, analisis lalu lintas jaringan, serta pengujian penetrasi terbatas. Metode penelitian dilakukan melalui beberapa tahapan, yaitu instalasi lingkungan pengujian, konfigurasi alat keamanan, pengumpulan data serangan simulasi, analisis hasil pemindaian, serta evaluasi efektivitas sistem pertahanan yang diterapkan. Hasil penelitian menunjukkan bahwa Kali Linux mampu mengidentifikasi berbagai jenis potensi ancaman, seperti kerentanan berisiko rendah hingga menengah, anomali pada protokol, dan konfigurasi jaringan yang tidak aman. Selain itu, sistem keamanan yang diterapkan berhasil meningkatkan tingkat deteksi serta mengurangi celah yang dapat dimanfaatkan oleh penyerang. Kesimpulan dari penelitian ini adalah bahwa penerapan sistem keamanan berbasis Kali Linux terbukti efektif sebagai langkah pencegahan serangan siber dan dapat menjadi model pertahanan yang dapat dikembangkan lebih lanjut untuk kebutuhan institusi maupun organisasi yang memprioritaskan keamanan data digital.

Abstrak: This research was conducted in response to the increasing intensity and complexity of cyberattacks that have the potential to compromise the integrity, confidentiality, and availability of data in various modern information systems. Institutions and organizations that increasingly rely on digital data require protection mechanisms that are not only reactive but also proactive. Therefore, this research implements a Kali Linux-based data security system as a comprehensive solution because this distribution provides various security tools such as Nmap, OpenVAS, and Snort that can be used to detect, analyze, and prevent cyberattacks. The main objective of this research is to design a security system capable of increasing network resilience through the application of vulnerability scanning techniques, network traffic analysis, and limited penetration testing. The research method is carried out through several stages, namely installing a test environment, configuring security tools, collecting simulated attack data, analyzing scan results, and evaluating the effectiveness of the implemented defense system. The results show that Kali Linux is able to identify various types of potential threats, such as low- to medium-risk vulnerabilities, protocol anomalies, and insecure network configurations. In addition, the implemented security system successfully increased the detection rate and reduced vulnerabilities that could be exploited by attackers. The conclusion of this study is that the implementation of a Kali Linux-based security system has proven effective as a measure to prevent cyber attacks and can be a defense model that can be further developed for the needs of institutions and organizations that prioritize digital data security.

PENDAHULUAN

Perkembangan teknologi informasi telah menghasilkan peningkatan signifikan dalam pemrosesan, penyimpanan, dan distribusi data pada berbagai bidang. Namun, perkembangan tersebut juga menyebabkan meningkatnya risiko terhadap serangan siber yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data.(Rongcai et al., n.d.) Berbagai jenis ancaman, termasuk malware, serangan jaringan, dan eksploitasi kerentanan, menunjukkan bahwa sistem informasi membutuhkan mekanisme perlindungan yang terstruktur dan dapat diandalkan. Kondisi ini

menuntut pendekatan keamanan yang sistematis serta penggunaan perangkat pendukung yang mampu mendeteksi dan mencegah potensi gangguan secara efektif.

Kali Linux merupakan salah satu distribusi sistem operasi yang dirancang untuk mendukung kegiatan analisis keamanan dan pengujian penetrasi. Distribusi ini menyediakan berbagai alat,

E-ISSN : 2776-9666
P-ISSN : 2776-1789

seperti Snort, Nmap, dan Metasploit, yang dapat digunakan untuk mengidentifikasi kerentanan, memetakan struktur jaringan, serta menganalisis potensi serangan.(Adamsyach Prana Walidin, Fahra Pebiana Putri, 2025) Kemampuannya dalam menyediakan lingkungan kerja yang terstandarisasi memungkinkan proses analisis keamanan dilakukan secara lebih konsisten dan terukur. Oleh karena itu, pemanfaatan Kali Linux menjadi relevan untuk mendukung upaya penguatan keamanan data.(Syahib et al., 2023)

Penelitian ini disusun untuk mengimplementasikan sistem keamanan data berbasis Kali Linux dalam konteks pencegahan serangan siber pada jaringan berskala kecil hingga menengah. Penelitian ini mencakup proses konfigurasi, pengujian, dan evaluasi terhadap efektivitas alat keamanan yang digunakan. Pendekatan ini dimaksudkan untuk memberikan gambaran empiris mengenai kemampuan Kali Linux dalam meningkatkan ketahanan sistem terhadap potensi ancaman, serta mengidentifikasi komponen pertahanan yang perlu diperkuat.

Dengan meningkatnya ketergantungan pada pemanfaatan data digital, keberadaan mekanisme keamanan yang terintegrasi menjadi aspek penting dalam menjaga keberlangsungan operasional.(Tommy et al., 2025) Oleh karena itu, penelitian ini diharapkan dapat menghasilkan temuan yang dapat digunakan sebagai rujukan dalam perancangan strategi keamanan data berbasis perangkat open-source. Selain itu, hasil penelitian ini diharapkan dapat mendukung pengembangan prosedur standar dalam penerapan keamanan jaringan pada berbagai jenis institusi atau lingkungan kerja.

KAJIAN PUSTAKA

a. Keamanan Data

Keamanan data merupakan suatu pendekatan terstruktur yang bertujuan menjaga kerahasiaan, integritas, dan ketersediaan informasi dalam suatu sistem.(Laksana et al., 2024) Konsep ini mencakup perlindungan terhadap akses tidak sah, pencegahan perubahan data yang tidak diinginkan, serta pemastian bahwa data tetap dapat digunakan ketika diperlukan. Penerapan keamanan data melibatkan penggunaan kebijakan, perangkat lunak, mekanisme kontrol akses, dan teknologi pertahanan untuk mengurangi risiko yang berpotensi mengganggu keberlangsungan operasional sistem informasi.

b. Serangan Siber

Serangan siber mencakup berbagai upaya yang dilakukan untuk mengakses, memodifikasi, mengganggu, atau merusak sistem dan data secara digital. Jenis serangan dapat berupa eksploitasi kerentanan, penyebaran malware, serangan berbasis jaringan, maupun serangan

yang ditujukan untuk membebani sistem.(Adi Saputra et al., 2023) Meningkatnya kompleksitas jaringan menyebabkan ancaman siber menjadi lebih variatif, sehingga diperlukan sistem pertahanan yang mampu mendeteksi dan merespons aktivitas mencurigakan secara cepat dan akurat.

c. Keamanan Sistem Informasi

Keamanan sistem informasi (KSI) adalah proses melindungi sistem informasi dari ancaman dan risiko yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data.(Santoso, 2023) KSI bertujuan untuk memastikan bahwa informasi yang disimpan, diproses, dan dikirimkan melalui sistem informasi tetap aman dan tidak dapat diakses oleh pihak yang tidak berwenang. Keamanan sistem informasi meliputi beberapa aspek, yaitu kerahasiaan, integritas, ketersediaan, autentikasi, dan otorisasi. Kerahasiaan berarti melindungi data dari akses yang tidak berwenang, sedangkan integritas berarti melindungi data dari perubahan atau penghapusan yang tidak berwenang.

Keamanan sistem informasi dapat diimplementasikan melalui beberapa cara, seperti firewall, enkripsi, antivirus, sistem deteksi intrusi, dan pengawasan serta pemantauan. Firewall dapat mengblokir akses yang tidak berwenang ke sistem informasi, sedangkan enkripsi dapat mengenkripsi data untuk melindungi dari akses yang tidak berwenang.(Dewi et al., 2025) Antivirus dapat mendeteksi dan menghapus malware yang dapat membahayakan sistem informasi, dan sistem deteksi intrusi dapat mendeteksi dan mencegah serangan yang tidak berwenang. Pengawasan dan pemantauan dapat memantau aktivitas sistem informasi untuk mendeteksi potensi ancaman. Dengan mengimplementasikan keamanan sistem informasi, organisasi dapat melindungi data dan sistem informasi mereka dari ancaman dan risiko, serta memastikan bahwa informasi yang disimpan dan diproses tetap aman dan dapat dipercaya.

d. Kali Linux

Kali Linux adalah sistem operasi yang menyediakan berbagai alat yang digunakan dalam kegiatan pemantauan keamanan, analisis kerentanan, dan pengujian penetrasi. Sistem ini dirancang untuk mendukung proses identifikasi ancaman dan evaluasi keamanan secara terstruktur. Dengan kelengkapan alat yang tersedia, Kali Linux memberikan lingkungan kerja yang memungkinkan analisis dilakukan secara lebih terstandardisasi dan efisien, sehingga relevan digunakan dalam implementasi sistem pertahanan jaringan.(Syafitri et al., 2024)

e. Analisis Kerentanan

Analisis kerentanan merupakan proses untuk mengidentifikasi kelemahan yang terdapat dalam sistem, jaringan, atau aplikasi.(Rahma, n.d.) Aktivitas ini dilakukan dengan memanfaatkan alat

pemindai, evaluasi konfigurasi, serta pengujian terhadap komponen sistem yang berpotensi menjadi titik masuk serangan. Hasil analisis kerentanan digunakan untuk menentukan tingkat risiko dan langkah perbaikan yang diperlukan agar sistem lebih tahan terhadap ancaman.(Hasibuan & Elhanafi, 2022)

METODE PENELITIAN

Penelitian ini merupakan penelitian eksperimental yang bertujuan untuk mengimplementasikan sistem keamanan data berbasis Kali Linux untuk mencegah serangan siber. Penelitian eksperimental ini akan dilakukan dengan menguji sistem keamanan data yang telah diimplementasikan pada sistem komputer yang umum digunakan.

a. Poulasi dan Sampel

Penelitian ini akan dilakukan pada sistem komputer yang umum digunakan, tanpa membedakan jenis sistem operasi, perangkat keras, atau perangkat lunak yang digunakan. Sampel penelitian ini akan dipilih secara acak dari populasi sistem komputer yang umum digunakan.

b. Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini adalah:

1. Kali Linux sebagai sistem operasi keamanan
2. Software keamanan seperti Snort, Nmap, dan Metasploit
3. Hardware seperti komputer dan jaringan

Instrumen-instrumen ini akan digunakan untuk mengimplementasikan sistem keamanan data dan melakukan pengujian keamanan pada sistem komputer.

c. Prosedur dan Teknik Penelitian

1. Instalasi Kali Linux: Instalasi Kali Linux pada sistem komputer yang akan digunakan sebagai server keamanan. Proses instalasi akan dilakukan dengan mengikuti prosedur yang telah ditentukan oleh pengembang Kali Linux.

2. Konfigurasi Keamanan: Konfigurasi keamanan pada Kali Linux, termasuk pengaturan firewall, IDS, dan IPS. Konfigurasi keamanan akan dilakukan dengan mengikuti *best practice* yang telah ditentukan oleh para ahli keamanan.

3. Pengujian Keamanan: Pengujian keamanan pada sistem komputer yang telah dikonfigurasi untuk memastikan bahwa sistem keamanan dapat berfungsi dengan baik. Pengujian keamanan akan dilakukan dengan menggunakan berbagai jenis serangan siber.

4. Simulasi Serangan: Simulasi serangan siber pada sistem komputer yang telah dikonfigurasi untuk memastikan bahwa sistem keamanan dapat mencegah serangan. Simulasi serangan akan dilakukan dengan menggunakan berbagai jenis serangan siber.

5. Analisis Hasil: Analisis hasil pengujian dan simulasi serangan untuk menentukan efektivitas sistem keamanan. Analisis hasil akan dilakukan dengan menggunakan teknik analisis data yang tepat.

d. Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif dan analisis statistik. Analisis deskriptif digunakan untuk menggambarkan karakteristik sistem keamanan, sedangkan analisis statistik digunakan untuk menentukan efektivitas sistem keamanan.

HASIL DAN PEMBAHASAN

A. Konfigurasi Keamanan pada Kali Linux

Konfigurasi keamanan pada Kali Linux merupakan proses pengaturan dan optimalisasi sistem operasi untuk meningkatkan keamanan dan melindungi sistem dari serangan dan ancaman.(Karim et al., 2024) Salah satu komponen konfigurasi keamanan yang penting adalah *firewall*, yang berfungsi untuk mengontrol lalu lintas jaringan dan memblokir akses yang tidak sah. *Firewall* pada Kali Linux dapat diaktifkan dan dikonfigurasi menggunakan perintah ufw (*Uncomplicated Firewall*), yang memungkinkan pengaturan aturan untuk mengizinkan atau memblokir akses ke port tertentu, protokol, dan alamat IP. Selain itu, *Intrusion Detection System* (IDS) juga merupakan komponen penting dalam konfigurasi keamanan Kali Linux. IDS berfungsi untuk mendeteksi serangan dan ancaman pada jaringan, dan dapat diinstal dan dikonfigurasi menggunakan Snort. Snort merupakan IDS yang populer dan dapat diintegrasikan dengan sistem operasi Kali Linux.(Purnama et al., 2023) *Intrusion Prevention System* (IPS) juga dapat diinstal dan dikonfigurasi pada Kali Linux, yang berfungsi untuk mencegah serangan dan ancaman pada jaringan. Snort dapat diintegrasikan dengan sistem operasi Kali Linux untuk mencegah serangan dan ancaman dengan mode IPS. Dengan melakukan konfigurasi keamanan pada Kali Linux, termasuk pengaturan firewall, IDS, dan IPS, dapat meningkatkan keamanan sistem dan melindungi dari serangan dan ancaman.

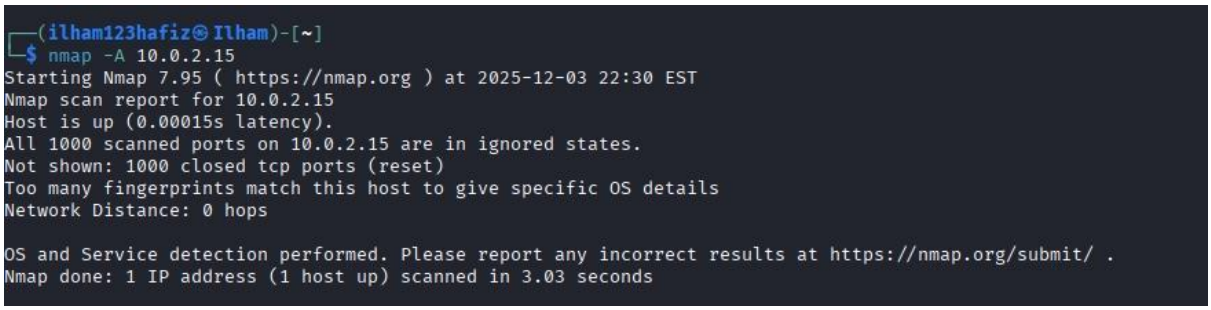
Gambar 1. Konfigurasi *Default* pada *Firewall*

Pada tampilan keluaran perintah sudo ufw status *verbose* terlihat bahwa sistem *firewall* UFW berada dalam kondisi aktif dan berfungsi sebagai mekanisme pengendalian akses jaringan pada sistem. Konfigurasi default memperlihatkan bahwa seluruh koneksi masuk (*incoming traffic*) ditetapkan ke dalam kebijakan *deny*, sedangkan seluruh koneksi keluar (*outgoing traffic*) diizinkan tanpa pembatasan. *Logging firewall* juga diaktifkan pada tingkat rendah untuk mendukung proses *monitoring* insiden. Berdasarkan aturan yang ditampilkan, sistem mengizinkan koneksi masuk pada port 22/TCP (SSH), 80/TCP (HTTP), dan 443/TCP (HTTPS), yang merupakan layanan esensial untuk pengelolaan sistem dan penyediaan layanan

web. Selain itu, terdapat aturan tambahan yang secara khusus menolak akses dari alamat IP 192.168.1.50, yang menunjukkan adanya penerapan kontrol berbasis sumber lalu lintas (*source-based filtering*). Seluruh aturan tersebut turut direplikasi ke dalam protokol IPv6 sehingga kebijakan keamanan diterapkan secara konsisten pada kedua versi protokol jaringan. Secara keseluruhan, konfigurasi ini menunjukkan bahwa sistem telah menerapkan kebijakan penyaringan lalu lintas yang ketat namun tetap memberikan akses terhadap layanan yang diperlukan, sehingga mendukung peningkatan keamanan jaringan secara menyeluruh.

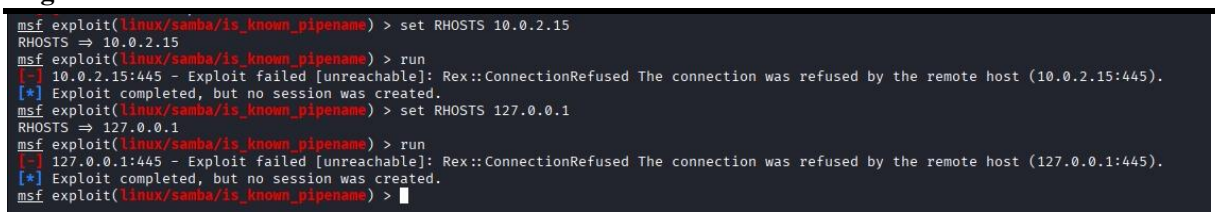
B. Pengujian Keamanan pada Sistem Komputer

Pengujian sistem keamanan dengan Nmap dan Metasploit bertujuan untuk mengevaluasi efektivitas konfigurasi keamanan yang telah diterapkan pada sistem komputer berbasis Kali Linux.(Fauzi & Hamdan, 2025) Pengujian ini dilakukan untuk memastikan bahwa mekanisme keamanan seperti *firewall, Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS) dapat berfungsi dengan baik dalam mendeteksi serta mencegah berbagai bentuk aktivitas berbahaya. Nmap digunakan untuk melakukan pemindaian port, layanan, dan sistem operasi guna melihat apakah masih terdapat port terbuka, layanan rentan, atau konfigurasi yang tidak aman setelah sistem dikunci. Hasil pemindaian ini membantu menilai apakah firewall dan aturan keamanan bekerja sesuai dengan desain. Metasploit digunakan untuk melakukan simulasi serangan siber terkontrol. Serangan ini bukan untuk merusak sistem, melainkan untuk memastikan bahwa IDS mampu mendeteksi upaya scanning, mencatat anomali jaringan, memberikan peringatan (*alert*) dalam mode IPS, serta mampu memblokir serangan secara otomatis.(Suhendi & Cahyo, 2021)



Gambar 2. Pengujian Keamanan dengan Nmap

Hasil pemindaian yang ditunjukkan pada gambar 2. merupakan keluaran dari perintah nmap -A 10.0.2.15, yang berfungsi untuk melakukan deteksi layanan, versi, dan sistem operasi pada host target. Berdasarkan hasil pemindaian tersebut, sistem mendeteksi bahwa *host* dengan alamat IP 10.0.2.15 berada dalam kondisi aktif, yang ditunjukkan oleh latensi respons yang sangat rendah, yaitu 0.000155 detik. Seluruh 1000 port yang dipindai berada dalam keadaan tertutup (*closed*), sehingga tidak ditemukan layanan jaringan yang terbuka dan siap menerima koneksi. Kondisi ini menunjukkan bahwa *host* telah menerapkan konfigurasi keamanan yang ketat, misalnya *firewall* aktif atau tidak menjalankan layanan jaringan apa pun. Nmap juga tidak mampu mengidentifikasi jenis sistem operasi secara spesifik karena terlalu banyak *fingerprints* yang cocok dengan karakteristik host tersebut, sehingga informasi OS tidak dapat ditentukan. Jarak jaringan terdeteksi sebesar 0 hops, yang menandakan bahwa proses pemindaian dilakukan dari segmen jaringan yang sama dengan target. Secara keseluruhan, hasil ini menunjukkan bahwa permukaan serangan (*attack surface*) pada *host* sangat minimal, karena tidak ada port terbuka yang dapat dieksploitasi oleh pihak tidak berwenang.



Gambar 3. Pengujian Keamanan dengan Metasploit

Pada gambar 3. menunjukkan hasil pengujian serangan menggunakan Metasploit *Framework* dengan modul linux/samba/is_known_pipename. Pada tahap ini, peneliti mencoba melakukan eksploitasi terhadap host target dengan alamat IP 10.0.2.15 dan port 445, yaitu port standar layanan SMB. Ketika proses exploit dijalankan, sistem memberikan keluaran berupa pesan "*ConnectionRefused: The connection was refused by the remote host*", yang mengindikasikan bahwa koneksi ke port 445 pada host target tidak dapat dilakukan. Kondisi tersebut menunjukkan bahwa layanan SMB tidak berjalan pada sistem target, atau akses ke port tersebut telah diblokir oleh konfigurasi *firewall* yang aktif. Percobaan kedua dilakukan terhadap alamat lokal 127.0.0.1 untuk memastikan apakah modul eksploit dapat berfungsi pada lingkungan yang sama. Namun, hasilnya tetap menunjukkan penolakan koneksi pada port yang sama, sehingga sesi eksploitasi tidak dapat dibuat. Secara keseluruhan, hasil pengujian ini memperlihatkan bahwa upaya eksploitasi tidak berhasil karena permukaan serangan yang dibutuhkan dalam hal ini layanan SMB pada port 445 tidak tersedia atau telah diamankan, sehingga sistem target tidak rentan terhadap jenis serangan yang memanfaatkan modul eksploit tersebut.

KESIMPULAN DAN SARAN

Implementasi sistem keamanan data berbasis Kali Linux terbukti efektif dalam mencegah serangan siber melalui kombinasi firewall, IDS/IPS, serta pengujian kerentanan menggunakan Nmap dan Metasploit. Hasil pemindaian menunjukkan seluruh port dalam kondisi tertutup dan tidak ditemukan layanan rentan yang dapat dieksploitasi. Pengujian eksploitasi juga gagal dilakukan karena koneksi ditolak oleh sistem, yang menandakan konfigurasi keamanan berjalan sesuai fungsinya. Secara keseluruhan, Kali Linux berhasil meningkatkan ketahanan sistem terhadap ancaman jaringan dan memberikan perlindungan yang memadai selama proses pengujian.

DAFTAR RUJUKAN

Adamsyach Prana Walidin, Fahra Pebiana Putri, D. K. (2025). Kali Linux Sebagai Alat Analisis Keamanan Jaringan Melalui. *Jurnal Mahasiswa Teknik Informatika*, *9*(1), 1188–1196.

Adi Saputra, L., Muhammad Akbar, F., Cahyaningtias, F., Puspa Ningrum, M., & Fauzi, A. (2023). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Jurnal Pendidikan Siber Nusantara*, *1*(2), 58–66. https://doi.org/10.38035/jpsn.v1i2.48

Dewi, A. K., Sibarani, B. K., Saputra, E., Norazlina, N., Susanti, S., Syafira, Y., &

Munakalla, Y. (2025). Strategi Efektif Pengendalian Internal dalam Keamanan Sistem Informasi Akuntansi untuk Perlindungan Data Keuangan. *Jurnal Ilmiah Raflesia Akuntansi*, *11*(1), 138–148. https://doi.org/10.53494/jira.v11i1.838

Fauzi, Y., & Hamdan, R. A. (2025). Pendekatan Metodologis dalam Deteksi Ancaman Siber pada Server Hosting Menggunakan NMAP dan Metasploit. *Sudo Jurnal Teknik Informatika*, *4*(1), 1–10. https://doi.org/10.56211/sudo.v4i1.868

Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. *Sudo Jurnal Teknik Informatika*, *1*(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

Karim, A., Umam, M. N., Fatahillah, M. L., & Hadi, M. A. F. (2024). the Identifikasi Kerentanan dan Upaya untuk Melindungi Data Pada Aplikasi Seluler. *JUSTIFY : Jurnal Sistem Informasi Ibrahimy*, *2*(2), 178–181. https://doi.org/10.35316/justify.v2i2.4159

Laksana, T. G., Mulyani, S., Komputer, I., Informatika, J., & Bhayangkara, U. (2024). *UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN Contact : Cite This Article : 3*(1), 109–122.

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. *Jurnal Teknologi Informasi Dan Komunikasi*, *14*(2), 358–369. https://doi.org/10.51903/jtikp.v14i2.726

Rahma, S. A. (n.d.). *Safety Use of Sil (Laboratory Information System) in Maintaining Patient Data Keamanan Penggunaan Sil (Sistem Informasi Laboratorium) Dalam Menjaga Kerahasiaan Data Pasien*. 1–19.

Rongcai, R. E. N., Guoxiong, W. U., & Ming, C. A. I. (n.d.). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*.

Santoso, T. J. (2023). *Teknologi Keamanan Siber* (Vol. 1).

Suhendi, H., & Cahyo, W. D. (2021). Perancangan dan Implementasi Keamanan Jaringan Menggunakan Snort sebagai Intrusion Prevention System (IPS) pada Jaringan Internet STEI ITB. *Naratif : Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, *3*(2), 60–68. https://naratif.sttbandung.ac.id/index.php/naratif/article/view/137

Syafitri, N., Lamada, M. S., & Suhardi, I. (2024). Implementasi Firewall untuk Mencegah Ancaman Keamanan pada Akses Remote Dekstop Protocol di Sistem Operasi Windows. *JIMU:Jurnal Ilmiah Multidisipliner*, *2*(04), 1095–1105.

https://doi.org/10.70294/jimu.v2i04.494

Syahib, M. I., Yasin, M. A., & Rauf, B. W. (2023). Pengenalan dan Instalasi Kali Linux untuk Langkah Awal Pengetahuan Tentang Keamanan Sistem Informasi. *Anoa: Jurnal Pengabdian Masyarakat Fakultas Teknik*, *1*(02), 32–38. https://doi.org/10.51454/anoa.v1i02.275

Tommy, S., Irwan, M., & Nasution, P. (2025). *EVALUASI MANAJEMEN RISIKO KEAMANAN SIBER PADA INFRASTRUKTUR DIGITAL PEMERINTAH : STUDI KASUS PUSAT DATA NASIONAL (PDN) Prodi Manajemen , Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sumatera Utara I . Pendahuluan Dalam era transformasi digital yang semakin pesat , data telah menjadi aset strategis dan fundamental bagi organisasi , baik di sektor publik maupun swasta . Pemerintah Indonesia melalui kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) mendorong digitalisasi layanan publik untuk menciptakan birokrasi yang efisien , transparan , dan akuntabel . Dalam kerangka ini , keberadaan Pusat Data Nasional (PDN) memegang peran krusial sebagai infrastruktur utama yang menghimpun , menyimpan , dan mengelola data dari ratusan instansi pemerintahan secara terpusat . Namun , seiring meningkatnya digitalisasi , kompleksitas risiko yang dihadapi juga bertambah , terutama dalam bentuk ancaman keamanan siber yang semakin canggih dan terorganisir . Salah satu peristiwa yang menandai krisis keamanan digital nasional adalah insiden kebocoran data PDN pada Juni 2024 , yang disebabkan oleh serangan ransomware LockBit Serangan ini tidak hanya menyebabkan lumpuhnya layanan publik di berbagai sektor , tetapi juga mengungkapkan kelemahan struktural dalam manajemen keamanan informasi pemerintah , seperti lemahnya kontrol akses , ketiadaan sistem pencadangan (backup), dan minimnya kesiapan dalam menangani insiden siber secara terkoordinasi . Padahal , keberhasilan sistem digital pemerintahan tidak hanya ditentukan oleh ketersediaan infrastruktur*. *04*(01), 1–26.