ISSN: XXXX-XXXX, Volume 1 Issue 1 (2025) Pages 32-40

JURNAL SINTIKA

Jurnal Sistem Informasi, Teknik Informatika, dan Sistem Komputer
Published by Yasin Publisher (Yayasan Amal Sosial Islami Nahdliyin)
Journal homepage: https://yasinpublisher.org/
https://doi.org/xx.xxxxx/xxxxxxx

Perancangan Keamanan Jaringan untuk Perlindungan Data Pemilu di Badan Pengawas Pemilihan Umum Kabupaten Kuantan Singingi

Amanda Zalva

Program Studi Teknik Informatika, Universitas Islam Kuantan Singingi, Indonesia
*Correspondence: E-mail: zalvaamanda15@gmail.com

Abstrak

Permasalahan utama yang dihadapi oleh Bawaslu Kabupaten Kuantan Singingi terkait keamanan data pemilu adalah adanya ancaman serangan siber, Saat ini, infrastruktur teknologi informasi di Bawaslu Kuantan Singingi belum sepenuhnya mampu menghadapi serangan-serangan tersebut, yang berpotensi mengakibatkan kebocoran data dan manipulasi hasil pemilu. Selain itu, keterbatasan dalam sistem keamanan jaringan yang digunakan memperbesar risiko terhadap integritas dan kepercayaan publik pada hasil pemilu. Tujuan dari laporan ini adalah untuk melakukan perancangan sistem informasi jaringan untuk perlindungan data pemilu berbasis web untuk mengatasi serangan ciber. Metodologi yang digunakan melibatkan analisis kebutuhan keamanan, desain arsitektur sistem yang mencakup firewall, sistem deteksi intrusi (IDS), dan enkripsi data. Implementasi sistem dilakukan dengan menerapkan teknologi terbaru dan melakukan pengujian keamanan secara menyeluruh untuk memastikan ketahanan sistem terhadap berbagai serangan. Perancangan sistem informasi jaringan untuk perlindungan data pemilu berbasis web berhasil dalam mengatasi serangan siber yang mungkin terjadi. Sistem yang dirancang mampu melindungi data pemilu dengan menerapkan langkah-langkah keamanan yang efektif, mendeteksi serangan secara dini, dan merespons dengan cepat. Namun, pemeliharaan dan pembaruan berkala tetap diperlukan untuk menghadapi ancaman yang terus berkembang dan memastikan sistem tetap aman dan berfungsi dengan optimal

Artikel Info

Article History:
Submitted/Received: 06/02/2025
First Revised: 12/02/2025
Accepted: 20/02/2025
Publication Date: 28/02/2025

Kata Kunci:
Bawaslu, Perlindungan Data Pemilu, Keamanan Siber, Sistem Informasi Jaringan, Enkripsi, Sistem Deteksi Intrusi (IDS).

1. Pendahuluan

Pemilu merupakan komponen penting dalam sistem demokrasi yang memungkinkan masyarakat untuk menentukan pemimpin mereka secara bebas dan adil. Di dalam proses pemilu, Badan Pengawas Pemilihan Umum (Bawaslu) memiliki peran krusial dalam mengawasi pelaksanaan pemilu agar berjalan sesuai dengan peraturan yang berlaku. Salah satu tanggung jawab utama Bawaslu adalah melindungi integritas data pemilu, yang mencakup informasi sensitif seperti data pemilih, hasil pemungutan suara, dan laporan pelanggaran. Di Kabupaten Kuantan Singingi, seperti di banyak daerah lain, Bawaslu dihadapkan pada berbagai tantangan dalam menjaga keamanan data pemilu tersebut.

Permasalahan utama yang dihadapi oleh Bawaslu Kabupaten Kuantan Singingi terkait keamanan data pemilu adalah adanya ancaman serangan siber, seperti peretasan, malware, dan pencurian data. Saat ini, infrastruktur teknologi informasi di Bawaslu Kuantan Singingi belum sepenuhnya mampu menghadapi serangan-serangan tersebut, yang berpotensi mengakibatkan kebocoran data dan manipulasi hasil pemilu. Selain itu, keterbatasan dalam sistem keamanan jaringan yang digunakan memperbesar risiko terhadap integritas dan kepercayaan publik pada hasil pemilu.

Kurangnya pemahaman dan kesadaran mengenai pentingnya keamanan data di kalangan staf dan pegawai juga menjadi permasalahan signifikan yang dihadapi Bawaslu Kabupaten Kuantan Singingi. Hal ini menyebabkan kelemahan dalam pengelolaan akses data dan penerapan protokol keamanan yang tepat. Selain itu, terbatasnya anggaran dan sumber daya untuk memperbarui teknologi dan sistem keamanan informasi menambah kompleksitas dalam upaya perlindungan data pemilu.

Dalam era digital yang penuh dengan ancaman siber, Bawaslu Kabupaten Kuantan Singingi memerlukan strategi keamanan jaringan yang andal untuk melindungi data-data tersebut. Salah satu metode yang potensial dalam menjaga keamanan jaringan adalah firewall port security, yang mampu membatasi akses jaringan hanya pada perangkat yang telah diverifikasi. Dengan penerapan metode ini, data Pemilu diharapkan terlindungi dari berbagai ancaman eksternal maupun internal, seperti akses tidak sah atau upaya peretasan.

Metodologi penelitian ini melibatkan beberapa tahapan penting, yaitu identifikasi kebutuhan keamanan, perancangan topologi jaringan, implementasi aturan port security pada firewall, pengujian keamanan melalui simulasi akses, analisis hasil pengujian, serta evaluasi akhir dan rekomendasi. Setiap tahapan dilakukan untuk memastikan bahwa metode firewall port security diterapkan secara optimal dalam konteks keamanan jaringan yang digunakan untuk data Pemilu di Bawaslu. Identifikasi kebutuhan dilakukan untuk memahami potensi ancaman dan kelemahan jaringan yang ada. Perancangan topologi jaringan berfokus pada desain yang membatasi akses perangkat tidak sah, sementara implementasi dan pengujian dilakukan untuk memverifikasi bahwa aturan keamanan berjalan sesuai yang diharapkan.

2. Metodologi

2.1 Pengambilan Data

Dalam penelitian ini, metode pengambilan data yang digunakan meliputi:

1) Observasi Lapangan

   Selama melakukan penelitian berlangsung peneliti mengamati dan mencari informasi tentang permasalahan yang dialami di BAWASLU Kuantan Singingi, salah satu permasalahan utama yang dialami oleh BAWASLU Kuantang Singingi adalah permasahalan keamanan jaringan terutama terkait keamanan data pemilu dan sayangnya pihak BAWASLU Kuantan Singingi belum mampu mencegah terjadinya kebocoran data nantinya. Setelah itu peneliti mengamati langsung infrastruktur jaringan dan sistem informasi yang ada di Badan Pengawas Pemilihan Umum Kabupaten Kuantan Singingi. Observasi mencakup identifikasi perangkat keras dan perangkat lunak yang digunakan, topologi jaringan, alur data, serta potensi titik kelemahan dalam keamanan jaringan.

DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX

2) Wawancara
   Peneliti melakukan wawancara dengan petugas teknis, administrator sistem, dan manajer keamanan IT di Badan Pengawas Pemilu. Wawancara bertujuan untuk mendapatkan informasi mendalam mengenai prosedur keamanan yang ada, potensi risiko yang dihadapi, serta kebutuhan dan harapan terhadap sistem keamanan jaringan yang akan dirancang.
3) Dokumentasi
   Peneliti mengumpulkan data dari dokumen internal yang relevan seperti kebijakan keamanan IT, laporan insiden keamanan sebelumnya, dan konfigurasi teknis jaringan yang ada. Data ini digunakan untuk memahami struktur jaringan saat ini, langkah-langkah keamanan yang telah diambil, dan masalah yang pernah terjadi
4) Studi Literatur
   Peneliti mencari referensi untuk pembuatan laporan dari berbagai sumber terpercaya seperti buku, jurnal, artikel ilmiah, standar keamanan jaringan, kebijakan pemerintah terkait keamanan data, serta pedoman dari Badan Pengawas Pemilu terkait perlindungan data pemilu. Data ini digunakan untuk memahami konsep, prinsip, dan praktik terbaik dalam keamanan jaringan serta kerangka regulasi dan standar yang berlaku.

2.2 Langkah-langkah Pengolahan Data

Berikut adalah langkah-langkah pengolahan data pada peneliti ini:

1) Identifikasi Kebutuhan Keamanan Data Pemilu: Peneliti melakukan identifikasi terhadap kebutuhan keamanan yang spesifik untuk melindungi data Pemilu. Ini mencakup identifikasi jenis data Pemilu yang perlu diamankan, perangkat yang terhubung ke jaringan, serta potensi ancaman yang mungkin dihadapi. Peneliti juga mengidentifikasi pengguna jaringan dan mengkaji potensi risiko, seperti peretasan atau akses ilegal.
2) Perancangan Topologi Jaringan untuk Perlindungan Data Pemilu: Berdasarkan kebutuhan yang telah diidentifikasi, peneliti merancang topologi jaringan dengan mengutamakan perlindungan data Pemilu. Peneliti memastikan firewall port security ditempatkan di titik-titik strategis untuk memproteksi lalu lintas data penting. Topologi ini didesain sedemikian rupa sehingga akses data Pemilu dibatasi hanya pada perangkat yang telah diverifikasi, meminimalkan risiko akses tidak sah.
3) Implementasi Aturan Port Security pada Firewall: Peneliti menerapkan aturan port security pada firewall untuk mengontrol akses ke data Pemilu. Peneliti mengonfigurasi port sehingga hanya perangkat resmi dari Bawaslu yang dapat mengakses data, sementara perangkat tidak sah akan diblokir. Peneliti mendokumentasikan konfigurasi aturan keamanan yang diterapkan, termasuk detail port dan perangkat yang diizinkan untuk mengakses data.
4) Pengujian Keamanan dengan Simulasi Akses Data Pemilu: Peneliti melakukan pengujian melalui simulasi akses untuk memastikan metode firewall port security bekerja efektif dalam melindungi data Pemilu. Dalam simulasi ini, peneliti mencoba mengakses jaringan dengan perangkat tidak terotorisasi untuk melihat apakah firewall berhasil mencegah akses tersebut, memastikan bahwa data tetap aman.
5) Analisis Hasil Pengujian Perlindungan Data Pemilu: Peneliti menganalisis hasil dari pengujian untuk menilai efektivitas metode firewall port security dalam melindungi data Pemilu. Peneliti mencatat hasil apakah perangkat tidak sah berhasil diblokir dan mengevaluasi apakah konfigurasi jaringan sudah memenuhi standar keamanan yang dibutuhkan untuk data Pemilu.
6) Evaluasi Akhir dan Rekomendasi untuk Penerapan Lebih Lanjut: Berdasarkan hasil analisis, peneliti melakukan evaluasi tentang efektivitas firewall port security dalam melindungi data Pemilu di Bawaslu. Jika terdapat kelemahan atau kebutuhan untuk

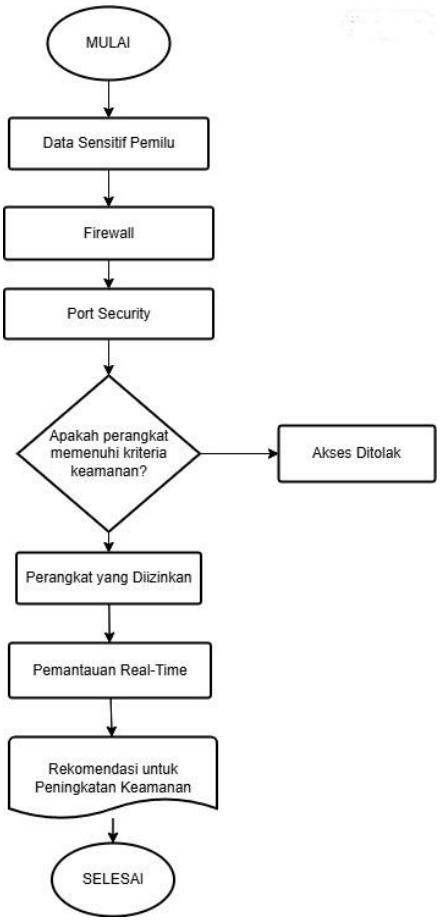
DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX

penyesuaian lebih lanjut, peneliti memberikan rekomendasi untuk peningkatan keamanan jaringan di masa depan. Peneliti menyusun kesimpulan yang mencakup efektivitas metode ini serta saran tambahan untuk penguatan keamanan jaringan.

3. Hasil dan Pembahasan

3.1 Flowchart Analisa Sistem Yang Sedang Berjalan

Pada sistem keamanan jaringan yang sedang berjalan, Bawaslu menggunakan metode perlindungan dasar yang bergantung pada firewall standar untuk mengamankan jaringan dan melindungi data Pemilu. Berikut adalah flowchart dari sistem keamanan jaringan yang sedang berjalan tersebut:

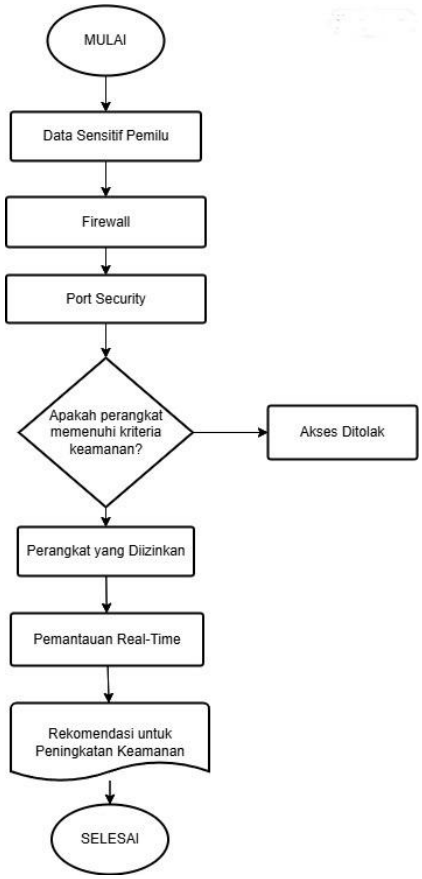


Gambar 1. Flowchart Sistem Informasi Yang Sedang Berjalan

3.2 Flowchart Sistem Yang di Usulkan

Dalam upaya melindungi data Pemilu yang bersifat sangat sensitif, Badan Pengawas Pemilihan Umum (Bawaslu) Kabupaten Kuantan Singingi membutuhkan sistem keamanan jaringan yang mampu menjaga kerahasiaan dan integritas data dari potensi ancaman. Data Pemilu yang mencakup informasi pemilih dan hasil perhitungan suara harus dilindungi secara ketat untuk memastikan kepercayaan publik terhadap proses Pemilu tetap terjaga. Salah satu pendekatan yang dapat diterapkan untuk memperkuat keamanan jaringan Bawaslu adalah metode firewall port security. Berikut ini adalah penjelasan mengenai penerapan, manfaat, serta efektivitas metode firewall port security dalam mengamankan data Pemilu yang dikelola oleh Bawaslu. Berikut merupakan flowchart analisa sistem yang diusulkan:

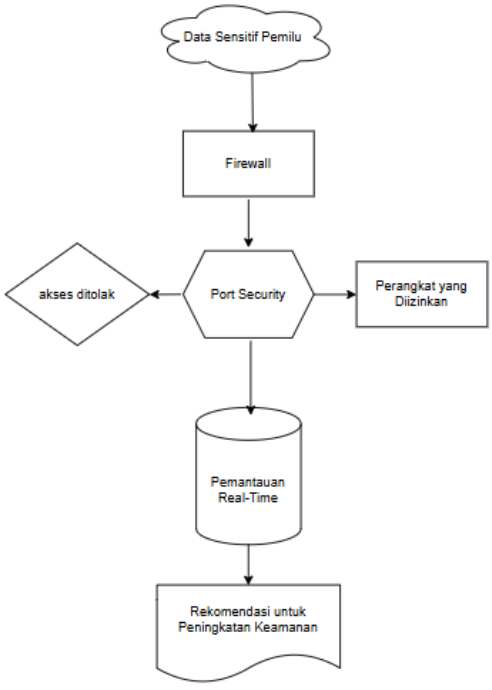
DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX



Gambar 2. Flowchart Sistem Yang di Usulkan

3.3 Blok Diagram

Adapun untuk sistem informasi jaringan yang ada di BAWASLU sebagai berikut :

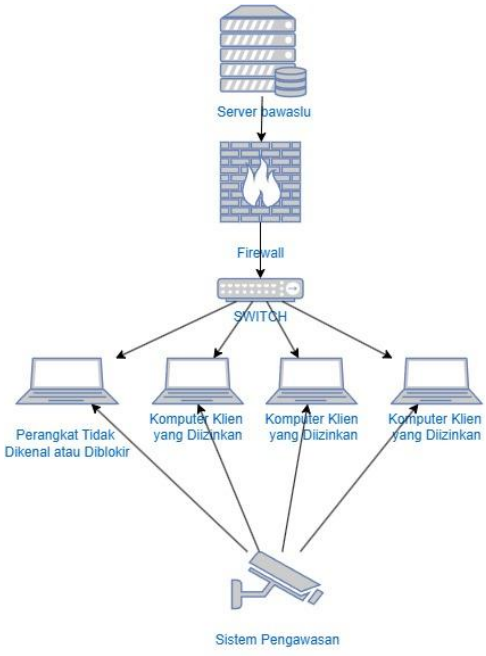


Gambar 3. Blok Diagram

DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX

3.4 Skema Jaringan

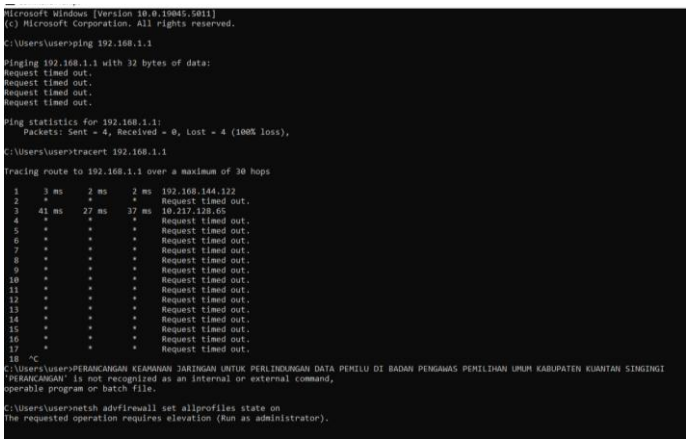
Skema jaringan (network diagram) adalah representasi visual yang menunjukkan struktur dan hubungan antar perangkat keras, perangkat lunak, serta koneksi dalam suatu jaringan komputer. Skema ini digunakan untuk memetakan bagaimana perangkat-perangkat seperti router, switch, server, komputer, dan perangkat lain saling terhubung melalui kabel atau secara nirkabel. Berikut merupakan skema jaringan untuk Rancang Bangun Sistem Informasi Keamanan Jaringan di Bawaslu Kabupaten Kuantan Singingi, Skema ini menjelaskan alur data dan interaksi antara berbagai komponen sistem untuk menjaga keamanan jaringan dalam perlindungan data pemilu :



Gambar 4. Skema Jaringan

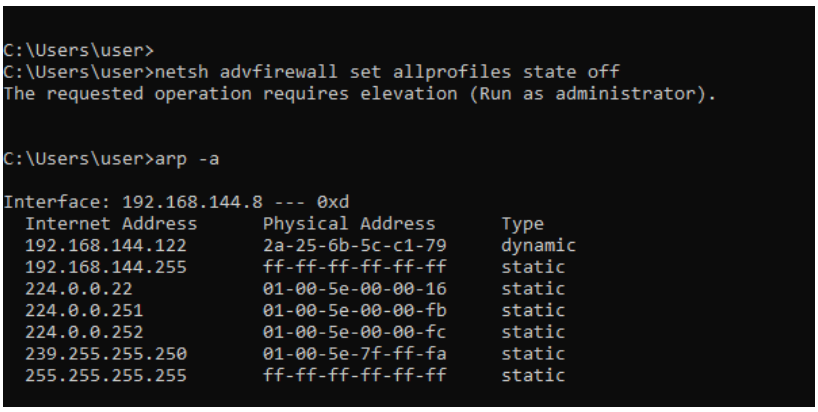
3.5 Konfigurasi Jaringan

Konfigurasi jaringan yang ditampilkan di bawah ini menunjukkan langkah-langkah yang diambil untuk memastikan komunikasi yang stabil dan aman antara perangkat di jaringan. Melalui penggunaan perintah ping dan traceroute, sistem dapat memverifikasi konektivitas dan mengidentifikasi rute yang dilalui data dari sumber ke tujuan. Proses ini sangat penting untuk memastikan kelancaran aliran data dan deteksi masalah dalam jaringan yang ada.



Gambar 5. Konfigurasi Jaringan 1

DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX



Gambar 6. Konfigurasi Jaringan 2

Berdasarkan hasil konfigurasi, berikut adalah analisis kesesuaian langkah-langkah tersebut dengan konsep perancangan keamanan jaringan :

1) Akses yang Diizinkan dan Diblokir:
   Pada gambar pertama, peneliti menggunakan perintah ping dan **tracert** untuk menguji konektivitas ke alamat **IP 192.168.1.1.** Hasil yang diperoleh menunjukkan "Request timed out," yang menandakan bahwa perangkat tidak dapat mengakses alamat tersebut. Hal ini sesuai dengan konsep Akses yang Diblokir, di mana firewall atau pengaturan keamanan jaringan lainnya, seperti port security pada switch, mencegah perangkat peneliti mencapai alamat tujuan. Jika perangkat klien yang sah memiliki akses ke server, perintah ping seharusnya berhasil tanpa menampilkan request timeout. Dengan demikian, hasil ini menunjukkan bahwa ada mekanisme yang memblokir akses, yang kemungkinan berasal dari pengaturan firewall atau aturan port security yang telah diterapkan.
2) Pemantauan Real-Time:
   Pada diatas, peneliti menggunakan perintah **arp -a** untuk menampilkan daftar perangkat dengan alamat IP dan alamat MAC yang pernah terhubung atau dikenali oleh komputer peneliti di jaringan. Konsep Pemantauan Real-Time di sini dapat mencakup pemeriksaan tabel ARP untuk memastikan bahwa tidak ada perangkat tidak dikenal yang terhubung ke jaringan. Namun, pemantauan real-time secara umum membutuhkan perangkat lunak khusus atau fitur monitoring yang lebih canggih, seperti Intrusion Detection System (IDS) atau Network Monitoring System, yang tidak sepenuhnya dapat dijalankan atau ditampilkan di Command Prompt. Tabel ARP **(arp -a)** hanya menyediakan informasi perangkat yang pernah berkomunikasi dengan komputer peneliti, bukan sebagai pemantauan berkelanjutan.
3) Konfigurasi Firewall:
   Pada gambar, peneliti mencoba menggunakan perintah **netsh advfirewall** untuk mengaktifkan atau menonaktifkan firewall. Namun, karena Command Prompt tidak dijalankan sebagai Administrator, perintah tersebut tidak berhasil dan menampilkan pesan "The requested operation requires elevation." Untuk melakukan konfigurasi firewall agar sesuai dengan perancangan yang ditetapkan (memblokir perangkat tidak dikenal), peneliti perlu membuka Command Prompt sebagai Administrator dan mengulang perintah netsh advfirewall set allprofiles state on atau off.

4. Simpulan

Perancangan sistem informasi jaringan untuk perlindungan data pemilu berbasis web berhasil dalam mengatasi serangan siber yang mungkin terjadi. Sistem yang dirancang mampu

DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX

melindungi data pemilu dengan menerapkan langkah-langkah keamanan yang efektif, mendeteksi serangan secara dini, dan merespons dengan cepat. Namun, pemeliharaan dan pembaruan berkala tetap diperlukan untuk menghadapi ancaman yang terus berkembang dan memastikan sistem tetap aman dan berfungsi dengan optimal. Secara keseluruhan, upaya awal peneliti dalam perancangan keamanan jaringan telah menunjukkan indikasi keberhasilan dalam memblokir akses tidak sah, sesuai dengan tujuan untuk melindungi data Pemilu. Hasil timeout pada perintah ping dan tracert menunjukkan fungsi firewall atau port security yang berhasil mencegah akses perangkat asing. Namun, untuk benar-benar mencapai perlindungan menyeluruh seperti yang tercantum dalam judul, peneliti masih memerlukan konfigurasi tambahan pada firewall serta sistem pemantauan real-time yang lebih canggih agar dapat mendeteksi dan menanggapi ancaman secara efektif.

5. Daftar Pustaka

Badan Pengawas Pemilihan Umum (Bawaslu). (2023). Tugas dan fungsi Bawaslu dalam penyelesaian sengketa pemilu. Jakarta: Bawaslu.

Badan Pengawas Pemilihan Umum (Bawaslu). (2023). Tugas dan wewenang Bawaslu dalam pengawasan pemilu. Jakarta: Bawaslu.

Badan Pengawas Pemilu Republik Indonesia. (2018). Tugas dan Fungsi Bawaslu dalam Pengawasan Pemilu. Jakarta: Bawaslu Press.

Badan Pengawas Pemilu Republik Indonesia. (2019). Tugas dan Wewenang Bawaslu dalam Pemilu. Jakarta: Bawaslu Press.

Badan Pengawas Pemilu Republik Indonesia. (2020). Peran Bawaslu dalam Pengawasan Pemilu. Jakarta: Bawaslu Press.

Bishop, M. (2023). Computer Security: Art and Science. Addison-Wesley.

Priyanto, I., & Kurniawan, R. (2021). Keamanan Jaringan Berbasis Firewall dalam Sistem Informasi E-Government. Jurnal Teknologi Informasi dan Komputer, 8(2), 45-54.

Putra, R. I. (2021). Keamanan Data dalam Sistem Pemilu di Kabupaten Kuantan Singingi: Tantangan dan Solusi. Jurnal Politik dan Keamanan, 12(3), 45-57.

Raharjo, S., & Putra, D. P. (2020). Analisis Keamanan Jaringan Menggunakan Metode IDPS pada Jaringan Perkantoran. Jurnal Informatika, 12(1), 22-33. https://doi.org/10.54321/jinfo.2020.12122

Republik Indonesia. (2007). Undang-Undang Nomor 22 Tahun 2007 tentang Penyelenggara Pemilu. Jakarta: Lembaran Negara Republik Indonesia.

Sari, R. P., & Widyanto, H. (2019). Penerapan Enkripsi Data untuk Meningkatkan Keamanan Jaringan Komputer. Jurnal Ilmiah Teknik Informatika, 10(3), 115-128.

Stallings, W. (2020). Network Security Essentials: Applications and Standards (6th ed.). Pearson.

Stallings, W. (2020). Network Security Essentials: Applications and Standards (6th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.

DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.

Wicaksono, A., & Setiawan, M. (2022). Sistem Keamanan Jaringan dalam Pengelolaan Data Pemilu Berbasis VPN dan Firewall. Jurnal Teknik Informatika dan Sistem Informasi, 14(2), 77-88.

DOI: https://doi.org/10.31078/jk19410
ISSN XXXX-XXXX