ANALISIS DAN IMPLEMENTASI SISTEM *FIREWALL* DAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *NDLC* PADA JARINGAN PERUMAHAN PAMULANG VILLAGE

Rahmad Raihan Amsyah[1], Nurhasanah[2]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Pamulang
Jalan Raya Puspitek No 46, Buaran, Kecamatan Pamulang, Kota Tangerang Selatan, Banten
rahmadraihanabung@gmail.com[1], dosen01123@unpam.ac.id[2],

Abstrak

Keamanan jaringan merupakan aspek penting dalam melindungi sumber daya jaringan dari berbagai ancaman siber. Penelitian ini bertujuan menganalisis dan mengimplementasikan sistem keamanan jaringan menggunakan *Firewall Mikrotik* dan *Intrusion Detection System (IDS)* berbasis *Snort* dengan metode *Network Development Life Cycle (NDLC)* pada jaringan Perumahan Pamulang Village. Sistem yang dibangun mengintegrasikan *Mikrotik* sebagai *Firewall*, *Snort* sebagai *IDS*, *Python* untuk mengolah log deteksi, *MySQL* sebagai basis data, serta aplikasi monitoring berbasis PHP untuk menampilkan informasi secara *real-time*. Pengujian dilakukan menggunakan *Black Box Testing*, *White Box Testing*, serta simulasi serangan berupa *Port Scanning*, *ICMP Flood*, dan *TCP Flood*. Hasil penelitian menunjukkan bahwa *Snort* mampu mendeteksi seluruh serangan yang diuji, sedangkan *Firewall Mikrotik* menjalankan aturan keamanan sesuai konfigurasi yang diterapkan. Selain itu, aplikasi monitoring mampu menampilkan log serangan secara *real-time* sehingga memudahkan *Administrator* dalam melakukan pemantauan keamanan jaringan. Implementasi sistem ini mendukung peningkatan kemampuan monitoring serta pengelolaan keamanan jaringan pada lingkungan penelitian.

Kata kunci : *Firewall*, *Intrusion Detection System (IDS)*, Keamanan Jaringan, *Network Development Life Cycle (NDLC)*, Monitoring Jaringan

Abstract

Network security is essential for protecting network resources from cyber threats. This study aims to analyze and implement a network security system using a Mikrotik Firewall and Snort-based Intrusion Detection System (IDS) following the Network Development Life Cycle (NDLC) method in the Pamulang Village residential network. The implemented system integrates Mikrotik as the Firewall, Snort as the IDS, Python for processing detection logs, MySQL as the database, and a PHP-based Web application for real-time monitoring. System evaluation was conducted through Black Box Testing, White Box Testing, and attack simulations including Port Scanning, ICMP Flood, and TCP Flood. The results show that Snort successfully detected all tested attacks, while the Mikrotik Firewall enforced the configured security rules to mitigate unauthorized access attempts. In addition, the Web-based monitoring application displayed attack logs in real time, enabling Administrators to monitor network security more effectively. The implementation demonstrates that the proposed system improves monitoring capability and supports network security management in the research environment.

Keywords*: Firewall, Intrusion Detection System (IDS), Network Security, Network Development Life Cycle (NDLC), Network Monitoring*

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong pemanfaatan jaringan komputer pada berbagai sektor, termasuk lingkungan perumahan. Seiring meningkatnya penggunaan jaringan, ancaman terhadap keamanan jaringan juga semakin beragam sehingga diperlukan mekanisme perlindungan yang mampu menjaga kerahasiaan, integritas, dan ketersediaan data. *Firewall* menjadi salah satu komponen penting dalam sistem keamanan jaringan karena mampu mengendalikan lalu lintas jaringan berdasarkan aturan yang telah ditetapkan (Tarina et al., 2026).
Selain *Firewall*, *Intrusion Detection System (IDS)* berperan dalam mendeteksi aktivitas yang mengindikasikan adanya serangan terhadap jaringan. *IDS* bekerja dengan memantau lalu lintas jaringan dan menghasilkan peringatan ketika ditemukan aktivitas yang mencurigakan, sehingga

Administrator dapat melakukan tindakan penanganan lebih cepat (Prisscilya et al., n.d.). Kombinasi antara *Firewall* dan *IDS* dapat meningkatkan efektivitas pengamanan jaringan karena tidak hanya membatasi akses yang tidak sah, tetapi juga mampu mendeteksi berbagai bentuk serangan yang terjadi pada jaringan (Hadi et al., 2026).

Berdasarkan hasil observasi di Perumahan Pamulang Village, pengelolaan jaringan masih dilakukan secara mandiri oleh masing-masing pengguna sehingga belum terdapat sistem keamanan dan monitoring yang terintegrasi. Kondisi tersebut menyebabkan proses pemantauan aktivitas jaringan belum berjalan secara optimal dan informasi mengenai serangan jaringan belum terdokumentasi dengan baik. Akibatnya, *Administrator* mengalami kesulitan dalam melakukan identifikasi maupun penanganan ketika terjadi gangguan atau serangan pada jaringan.

Untuk mengatasi permasalahan tersebut diperlukan suatu metode pengembangan yang mampu menghasilkan implementasi sistem keamanan secara terstruktur. *Network Development Life Cycle (NDLC)* merupakan metode yang menyediakan tahapan mulai dari analisis, perancangan, implementasi, hingga monitoring jaringan sehingga proses pembangunan sistem dapat dilakukan secara sistematis (Yulianto & Aprilyani, n.d.).

Berdasarkan uraian tersebut, penelitian ini mengimplementasikan sistem keamanan jaringan yang mengintegrasikan *Firewall Mikrotik* dan *Intrusion Detection System* berbasis *Snort* menggunakan metode *NDLC* pada jaringan Perumahan Pamulang Village. Selain itu, sistem dilengkapi dengan aplikasi monitoring berbasis *Web* yang mampu menampilkan log hasil deteksi serangan secara real-time sehingga memudahkan *Administrator* dalam melakukan pemantauan keamanan jaringan. Penelitian ini diharapkan dapat meningkatkan efektivitas pengamanan serta monitoring jaringan pada lingkungan penelitian.

PENELITIAN RELEVAN

Penelitian mengenai implementasi keamanan jaringan menggunakan Firewall dan Intrusion Detection System (IDS) telah banyak dilakukan. Dan et al. (n.d.) menerapkan Firewall berbasis IPTables menggunakan metode Network Development Life Cycle (NDLC) pada Dinas Perpustakaan dan Kearsipan Provinsi Bengkulu. Hasil penelitian menunjukkan bahwa penerapan Firewall mampu meningkatkan keamanan jaringan dengan membatasi akses yang tidak sesuai dengan kebijakan yang telah ditentukan.

Prisscilya et al. (n.d.) mengimplementasikan Intrusion Detection System (IDS) untuk mendeteksi aktivitas mencurigakan pada jaringan komputer PT Mega Esa Farm. Penelitian tersebut membuktikan bahwa IDS mampu memberikan informasi mengenai aktivitas serangan sehingga Administrator dapat melakukan tindakan penanganan lebih cepat.

Selanjutnya, Awal & Gusman (2023) mengembangkan sistem keamanan jaringan menggunakan kombinasi Snort sebagai Intrusion Detection System dan IPTables sebagai Intrusion Prevention System berbasis Linux. Hasil penelitian menunjukkan bahwa integrasi kedua teknologi tersebut mampu mendeteksi sekaligus mencegah berbagai bentuk serangan pada jaringan komputer.

Adzimi et al. (2024) mengimplementasikan konfigurasi Firewall dan *Intrusion Detection System* menggunakan Debian. Penelitian tersebut menunjukkan bahwa kombinasi kedua mekanisme keamanan mampu meningkatkan perlindungan jaringan melalui proses penyaringan lalu lintas dan deteksi aktivitas mencurigakan secara bersamaan.

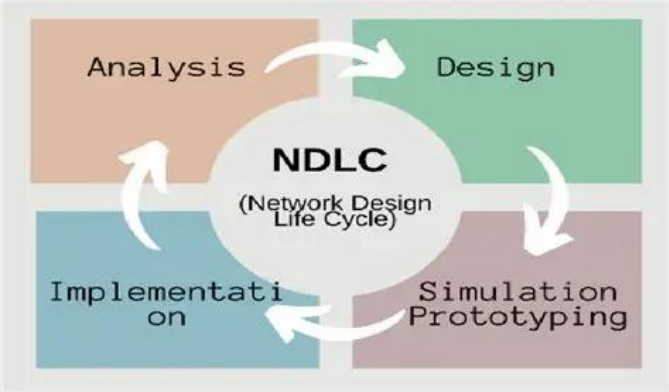
Berdasarkan beberapa penelitian tersebut, implementasi Firewall maupun IDS telah terbukti mampu meningkatkan keamanan jaringan. Namun, penelitian Dan et al. (n.d.) lebih berfokus pada penerapan Firewall berbasis IPTables, sedangkan Prisscilya et al. (n.d.), Awal & Gusman (2023), serta Adzimi et al. (2024) menitikberatkan pada deteksi dan/atau pencegahan serangan. Penelitian-penelitian tersebut belum secara spesifik mengintegrasikan Firewall Mikrotik, Snort IDS, pengolahan log, basis data, dan media monitoring berbasis web secara terpadu pada lingkungan jaringan perumahan. Oleh karena itu, penelitian ini mengintegrasikan Firewall Mikrotik, Snort IDS, Python, MySQL, serta aplikasi monitoring berbasis web menggunakan metode *Network Development Life Cycle* (NDLC) sehingga Administrator dapat melakukan pemantauan log serangan secara lebih efektif.

METODE PENELITIAN

Penelitian ini menggunakan metode *Network Development Life Cycle (NDLC)* sebagai tahapan dalam pengembangan sistem keamanan jaringan. Metode ini dipilih karena memiliki alur yang terstruktur, mulai dari analisis hingga monitoring, sehingga proses implementasi sistem dapat dilakukan secara sistematis.

Objek penelitian berada pada jaringan Perumahan Pamulang Village. Sistem keamanan yang dibangun mengintegrasikan *Mikrotik* sebagai *Firewall*, *Snort* sebagai *Intrusion Detection System (IDS)*, Python sebagai pengolah log deteksi, *MySQL* sebagai basis data, serta aplikasi monitoring berbasis *web* menggunakan PHP. Sistem dirancang untuk mendeteksi serangan *Port Scanning*, *ICMP Flood*, dan *TCP Flood*, kemudian menyimpan hasil deteksi ke dalam basis data sehingga dapat ditampilkan secara real-time pada halaman monitoring.

Tahapan penelitian diawali dengan proses analisis untuk mengidentifikasi kondisi jaringan, kebutuhan sistem, serta potensi ancaman yang dapat memengaruhi keamanan jaringan. Selanjutnya dilakukan tahap perancangan yang meliputi penyusunan topologi jaringan, arsitektur sistem, serta mekanisme komunikasi antara *Firewall*, *IDS*, basis data, dan aplikasi monitoring. Setelah rancangan selesai, dilakukan simulasi untuk memastikan konfigurasi yang telah dibuat dapat berjalan sesuai dengan kebutuhan sistem. Tahap implementasi dilakukan dengan mengonfigurasi seluruh perangkat dan aplikasi yang digunakan. Tahap terakhir adalah monitoring, yaitu melakukan pengamatan terhadap aktivitas jaringan serta log serangan yang dihasilkan oleh sistem.



Gambar 1. Tahapan *NDLC*

Pengujian sistem dilakukan menggunakan *Black Box Testing* dan *White Box Testing*. *Black Box Testing* digunakan untuk memastikan seluruh fungsi pada aplikasi monitoring berjalan sesuai dengan kebutuhan pengguna, sedangkan *White Box Testing* dilakukan untuk menguji logika program berdasarkan source code. Selain itu, dilakukan simulasi serangan menggunakan Nmap untuk *Port Scanning*, Hping3 untuk *ICMP Flood*, dan Hping3 untuk *TCP Flood* guna menguji kemampuan sistem dalam mendeteksi serangan serta menampilkan informasi log pada aplikasi monitoring.

Tabel 1. Skenario Pengujian Sistem

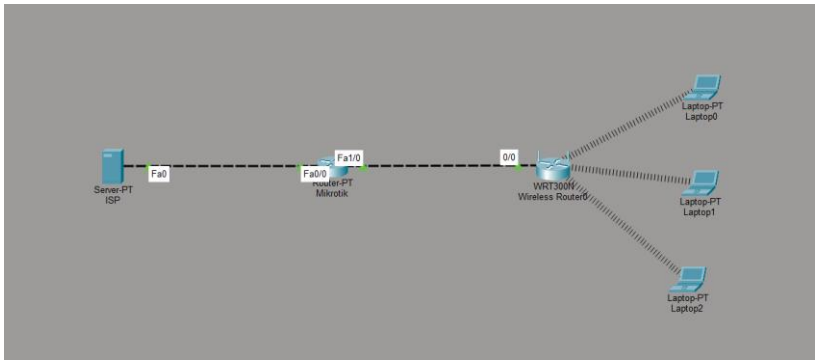
No	Jenis Pengujian	Skenario	Hasil yang Diharapkan
1	*Black Box Testing*	Menguji fungsi *Login Administrator*	*Administrator* dapat masuk ke sistem menggunakan username dan password yang valid.
2	*Black Box Testing*	Menguji fungsi *Dashboard*	*Dashboard* menampilkan informasi statistik dan menu utama dengan benar.
3	*Black Box Testing*	Menguji halaman *Monitor Log*	Data log serangan berhasil ditampilkan pada halaman monitoring.
4	*Black Box Testing*	Menguji fungsi *Logout*	Sistem berhasil mengakhiri sesi *Administrator* dan kembali ke halaman *Login*.
5	*White Box Testing*	Menguji alur logika program *Login*	Seluruh jalur eksekusi pada modul *Login* berjalan sesuai flow graph.
6	*White Box Testing*	Menguji alur logika program *Dashboard*	Seluruh jalur independen pada modul *Dashboard* dapat dieksekusi.
7	*White Box Testing*	Menguji alur logika program *Monitor Log*	Seluruh proses pengambilan dan penampilan data log berjalan sesuai alur program.
8	*White Box Testing*	Menguji alur logika program *Logout*	Proses penghapusan session dan pengalihan halaman berjalan sesuai logika program.

9	Simulasi Serangan	*Port Scanning* menggunakan Nmap	*Snort* mendeteksi aktivitas *Port Scanning* dan log serangan tersimpan pada database serta ditampilkan pada *Web* monitoring.
10	Simulasi Serangan	*ICMP Flood* menggunakan Hping3	*Snort* mendeteksi serangan *ICMP Flood* dan informasi serangan ditampilkan pada halaman monitoring.
11	Simulasi Serangan	*TCP Flood* menggunakan Hping3	*Snort* mendeteksi serangan *TCP Flood* dan log serangan berhasil ditampilkan pada aplikasi monitoring.

HASIL DAN PEMBAHASAN

Implementasi Topologi Jaringan

Implementasi sistem dilakukan pada jaringan Perumahan Pamulang Village dengan mengintegrasikan *Mikrotik* sebagai *Firewall*, server *Debian* sebagai *Intrusion Detection System (IDS)* menggunakan *Snort*, basis data *MySQL*, serta aplikasi monitoring berbasis *Web*. Seluruh perangkat saling terhubung sehingga proses deteksi serangan dapat dilakukan secara otomatis. Ketika terjadi aktivitas yang sesuai dengan aturan deteksi *Snort*, informasi serangan diproses oleh Python, disimpan ke dalam basis data, kemudian ditampilkan pada aplikasi monitoring secara real-time.

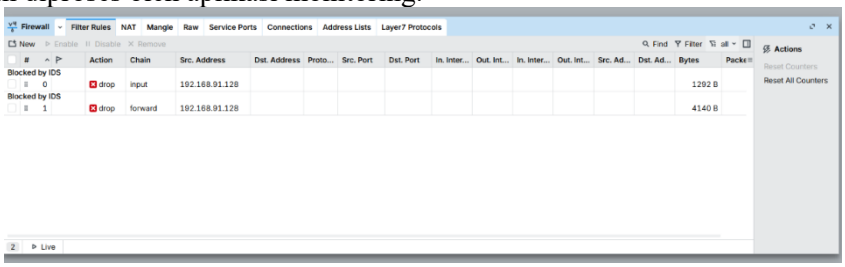


Gambar 2. Topologi Implementasi Sistem

Topologi jaringan yang diterapkan menghubungkan seluruh perangkat sehingga proses komunikasi antar komponen dapat berlangsung secara terintegrasi. Seluruh trafik jaringan terlebih dahulu melewati *Firewall Mikrotik* sebelum diteruskan menuju server *IDS*. Server *Debian* yang menjalankan *Snort* bertugas melakukan inspeksi terhadap paket data yang melintas berdasarkan rule yang telah dikonfigurasi. Selanjutnya, hasil deteksi diproses menggunakan Python dan disimpan ke dalam basis data *MySQL* sehingga informasi tersebut dapat ditampilkan pada aplikasi monitoring berbasis *Web* secara real-time. Pendekatan ini memudahkan *Administrator* dalam melakukan pemantauan keamanan jaringan dari satu antarmuka.

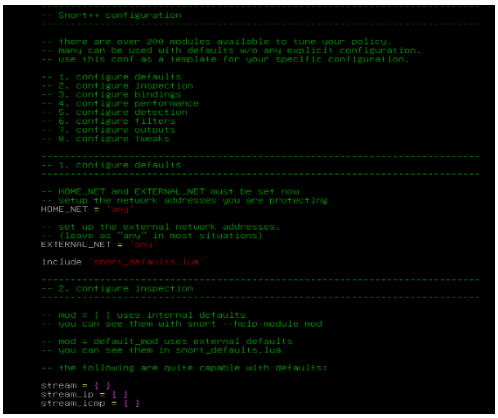
Implementasi *Firewall* dan *Intrusion Detection System*

Firewall Mikrotik dikonfigurasi menggunakan aturan filtering untuk mengendalikan lalu lintas jaringan dan membatasi akses yang tidak sesuai dengan kebijakan keamanan. Sementara itu, *Snort* dikonfigurasi menggunakan beberapa rule untuk mendeteksi aktivitas *Port Scanning*, *ICMP Flood*, dan *TCP Flood*. Ketika salah satu serangan terdeteksi, sistem secara otomatis menghasilkan log yang kemudian diproses oleh aplikasi monitoring.



Gambar 3. Konfigurasi *Firewall Mikrotik*

e-ISSN : 2715-8756

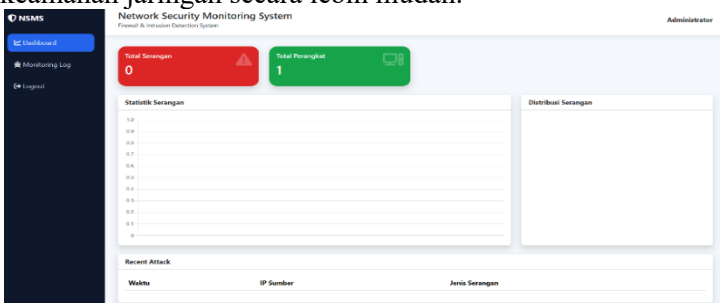


Gambar 4. Konfigurasi Rule *Snort IDS*

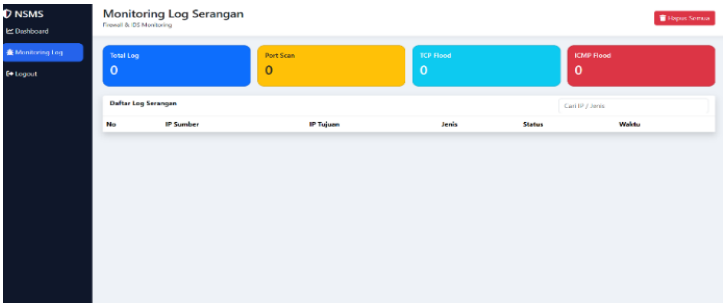
Rule *Snort* disusun berdasarkan karakteristik masing-masing jenis serangan yang diuji pada penelitian ini. Ketika pola paket sesuai dengan rule yang telah ditentukan, *Snort* secara otomatis menghasilkan alert sebagai indikator adanya aktivitas mencurigakan. *Alert* tersebut kemudian diproses oleh aplikasi sehingga informasi mengenai jenis serangan, alamat IP sumber, serta waktu kejadian dapat tersimpan ke dalam basis data. Mekanisme tersebut memungkinkan proses deteksi berlangsung secara otomatis tanpa memerlukan pengawasan manual secara terus-menerus.

Implementasi *Web* Monitoring

Aplikasi monitoring dikembangkan menggunakan PHP dengan basis data *MySQL* sebagai media penyimpanan log serangan. Halaman monitoring menampilkan informasi berupa alamat IP penyerang, jenis serangan, waktu kejadian, serta status hasil deteksi. Selain itu, *Dashboard* juga menyajikan ringkasan jumlah serangan berdasarkan kategori sehingga *Administrator* dapat memantau kondisi keamanan jaringan secara lebih mudah.



Gambar 5. *Dashboard* Monitoring



Gambar 6. Halaman *Monitor Log*

Halaman *Monitor Log* menjadi komponen utama pada aplikasi monitoring karena seluruh aktivitas serangan yang berhasil dideteksi akan ditampilkan pada halaman ini. Informasi yang disajikan meliputi alamat IP penyerang, jenis serangan, waktu kejadian, serta status deteksi. Penyajian data dalam bentuk tabel memudahkan *Administrator* dalam melakukan pencarian maupun analisis terhadap riwayat serangan yang terjadi pada jaringan.

Selain menampilkan data secara real-time, halaman monitoring juga mendukung proses dokumentasi aktivitas keamanan jaringan. Data yang tersimpan pada basis data dapat digunakan sebagai bahan evaluasi untuk mengetahui pola serangan yang paling sering terjadi sehingga

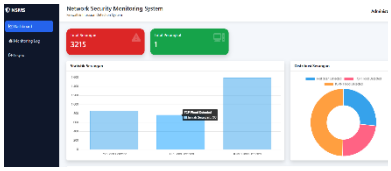
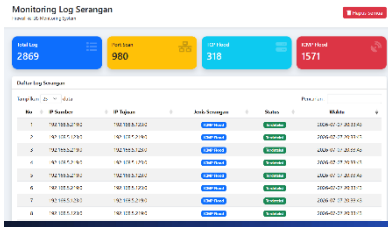
e-ISSN : 2715-8756

Administrator dapat melakukan penyesuaian terhadap konfigurasi *Firewall* maupun rule *IDS* apabila diperlukan.

Hasil Pengujian Sistem

Pengujian dilakukan menggunakan *Black Box Testing*, *White Box Testing*, serta simulasi serangan jaringan. *Black Box Testing* menunjukkan seluruh fungsi aplikasi, seperti *Login*, *Dashboard*, *Monitor Log*, dan *Logout*, berjalan sesuai dengan kebutuhan sistem. *White Box Testing* menghasilkan seluruh jalur independen pada setiap modul berhasil dieksekusi berdasarkan hasil perhitungan *Cyclomatic Complexity*.

Tabel 2. Hasil Pengujian *Black Box*

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	*Login* Admin	Sistem menampilkan halaman *Dashboard*		Berhasil
2.	Gagal *Login* Admin	Sistem menampilkan pesan kesalahan		Berhasil
3.	*Dashboard*	Statistik dan grafik serangan ditampilkan		Berhasil
4.	*Monitor Log*	Daftar log serangan ditampilkan		Berhasil
5.	*Logout*	Sistem kembali ke halaman *Login*		Berhasil

Tabel 3. Hasil Pengujian *White Box*

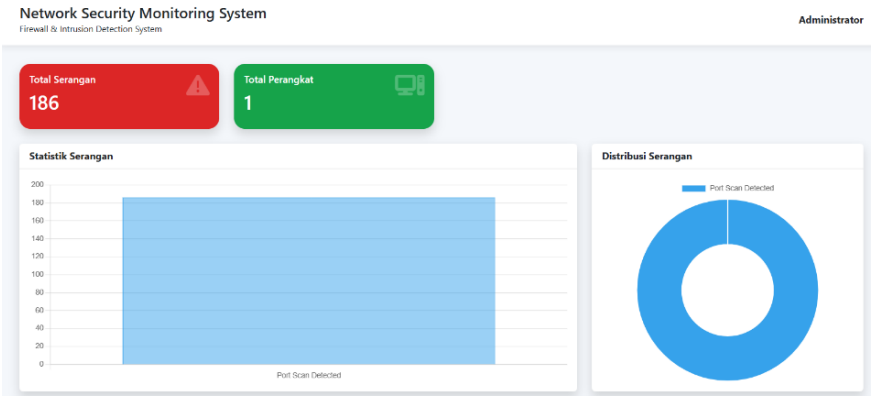
No	Modul	*Node*	*Edge*	*Cyclomatic Complexity*	*Independent Path*	Status
1	*Login*	7	7	2	2	Berhasil
2	*Dashboard*	7	9	4	4	Berhasil
3	*Monitor Log*	13	14	3	3	Berhasil
4	*Logout*	3	2	1	1	Berhasil

Berdasarkan hasil *Black Box Testing* dan *White Box Testing*, seluruh fungsi utama sistem dapat dijalankan sesuai dengan kebutuhan yang telah ditetapkan. Pengujian *Black Box* menunjukkan bahwa setiap fitur, mulai dari proses autentikasi hingga monitoring log serangan, memberikan keluaran yang sesuai dengan skenario pengujian. Sementara itu, hasil *White Box Testing* membuktikan bahwa seluruh jalur independen pada setiap modul berhasil dieksekusi berdasarkan nilai *Cyclomatic Complexity* yang diperoleh.

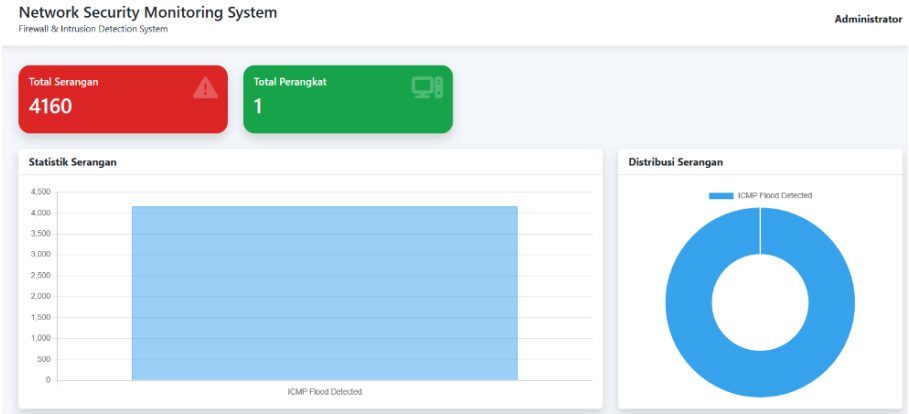
Keberhasilan kedua metode pengujian tersebut menunjukkan bahwa sistem tidak hanya memenuhi kebutuhan fungsional, tetapi juga memiliki alur logika program yang berjalan sesuai dengan

rancangan. Dengan demikian, aplikasi monitoring dapat digunakan sebagai media pengawasan keamanan jaringan yang mendukung proses deteksi dan pencatatan aktivitas serangan secara lebih efektif.

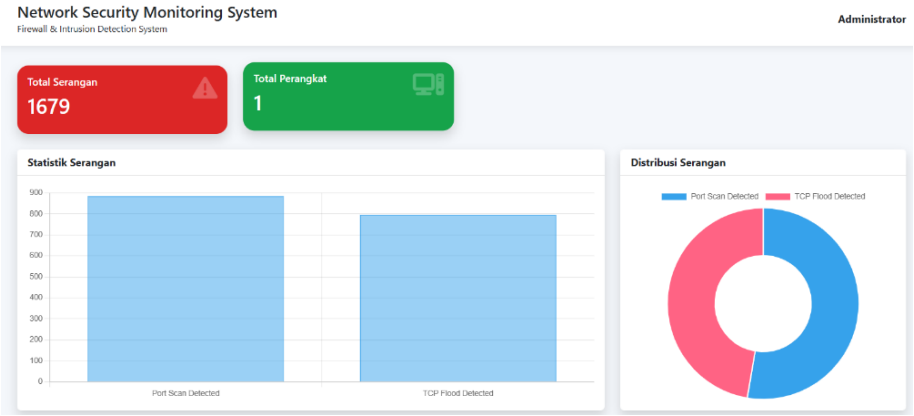
Selanjutnya dilakukan simulasi serangan menggunakan Nmap untuk *Port Scanning* serta Hping3 untuk *ICMP Flood* dan *TCP Flood*. Berdasarkan hasil pengujian, seluruh serangan berhasil dideteksi oleh *Snort* dan informasi hasil deteksi tersimpan pada basis data serta ditampilkan pada aplikasi monitoring secara real-time.



Gambar 7. Hasil Deteksi *Port Scanning*



Gambar 8. Hasil Deteksi *ICMP Flood*



Gambar 9. Hasil Deteksi *TCP Flood*

Untuk mengetahui efektivitas sistem, dilakukan rekapitulasi hasil pengujian terhadap setiap jenis serangan.

Tabel 4. Hasil Rekapitulasi Pengujian Serangan

Jenis Serangan	Status Deteksi *Snort*	Tersimpan di Database	Ditampilkan di *Web*
Port Scanning	Berhasil	Berhasil	Berhasil
ICMP Flood	Berhasil	Berhasil	Berhasil
TCP Flood	Berhasil	Berhasil	Berhasil

Rekapitulasi hasil pengujian memperlihatkan bahwa seluruh jenis serangan yang diuji berhasil dideteksi oleh *Snort* dan ditampilkan pada aplikasi monitoring. Hal ini menunjukkan bahwa integrasi antara *Firewall Mikrotik*, *Snort IDS*, Python, *MySQL*, dan aplikasi berbasis *Web* telah berjalan sesuai dengan rancangan sistem. Selain meningkatkan kemampuan deteksi, sistem juga mempermudah *Administrator* dalam memperoleh informasi keamanan jaringan secara cepat dan terpusat.

Hasil pengujian menunjukkan bahwa sistem keamanan yang dibangun mampu menjalankan fungsi *Firewall*, mendeteksi aktivitas serangan menggunakan *Snort*, serta menyajikan informasi hasil deteksi melalui aplikasi monitoring berbasis *Web*. Integrasi antar komponen sistem berjalan sesuai dengan rancangan sehingga *Administrator* dapat melakukan pemantauan kondisi keamanan jaringan secara lebih efektif dan terpusat.

Analisis Efektivitas Implementasi

Implementasi sistem keamanan jaringan yang mengintegrasikan *Firewall Mikrotik*, *Snort IDS*, Python, *MySQL*, dan aplikasi monitoring berbasis *Web* menunjukkan bahwa setiap komponen mampu menjalankan fungsinya secara terpadu. *Firewall* berperan dalam mengendalikan lalu lintas jaringan sesuai dengan aturan keamanan yang telah dikonfigurasi, sedangkan *Snort* melakukan analisis terhadap paket data yang melintas untuk mengidentifikasi aktivitas yang mengarah pada serangan. Seluruh hasil deteksi kemudian diproses dan disimpan ke dalam basis data sehingga dapat ditampilkan pada aplikasi monitoring tanpa memerlukan proses pencatatan secara manual.

Berdasarkan hasil pengujian yang telah dilakukan, aplikasi monitoring mampu menyajikan informasi serangan dalam bentuk yang mudah dipahami oleh *Administrator*. Informasi mengenai jenis serangan, alamat IP sumber, serta waktu terjadinya serangan dapat ditampilkan secara real-time sehingga proses pemantauan jaringan menjadi lebih efisien. Selain mempermudah proses identifikasi ketika terjadi gangguan, penyimpanan log pada basis data juga memberikan kemudahan dalam melakukan penelusuran riwayat serangan sebagai bahan evaluasi terhadap kebijakan keamanan jaringan yang telah diterapkan.

Secara keseluruhan, hasil implementasi menunjukkan bahwa integrasi antara mekanisme pencegahan melalui *Firewall* dan mekanisme pendeteksian menggunakan *IDS* mampu meningkatkan efektivitas pengamanan jaringan. Kehadiran aplikasi monitoring berbasis *Web* juga memberikan nilai tambah karena seluruh informasi keamanan dapat dipantau melalui satu antarmuka yang terpusat. Dengan demikian, *Administrator* tidak hanya memperoleh informasi mengenai adanya serangan, tetapi juga dapat melakukan analisis terhadap pola serangan yang terjadi sebagai dasar untuk meningkatkan konfigurasi keamanan pada jaringan di masa mendatang.

SIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, sistem keamanan jaringan yang mengintegrasikan *Firewall Mikrotik* dan *Intrusion Detection System (IDS)* berbasis *Snort* menggunakan metode *Network Development Life Cycle (NDLC)* berhasil diterapkan pada jaringan Perumahan Pamulang Village. Integrasi antara *Firewall*, *IDS*, basis data, dan aplikasi monitoring berbasis *Web* mampu membentuk mekanisme keamanan yang mendukung proses pemantauan jaringan secara terpusat.

Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi serangan berupa *Port Scanning*, *ICMP Flood*, dan *TCP Flood*, kemudian menyimpan serta menampilkan informasi log serangan secara real-time melalui aplikasi monitoring. Selain itu, hasil *Black Box Testing* dan *White Box Testing* menunjukkan bahwa seluruh fungsi aplikasi serta logika program berjalan sesuai dengan rancangan sistem. Dengan demikian, sistem yang dikembangkan dapat membantu *Administrator* dalam memantau aktivitas jaringan, mengidentifikasi indikasi serangan secara lebih cepat, serta meningkatkan efektivitas pengelolaan keamanan jaringan.

DAFTAR PUSTAKA

Adzimi, S. N. (2024). Implementasi Konfigurasi *Firewall* dan Sistem Deteksi Intrusi menggunakan *Debian*. *Journal of Internet and Software Engineering, 1*(4), 12. doi:https://doi.org/10.47134/pjise.v1i4.2681

Albar, R., & Putra, R. O. (2022). Analisis Keamanan Jaringan Menggunakan Metode Sniffing Dan Implementasi Keamanan Jaringan Pada *Mikrotik* Router OS V6.48.3 Menggunakan Metode Port Knocking. *Journal of Informatics and Computer Science (JICS), 8*(1), 1-11. doi:https://doi.org/10.33143/jics.Vol8.Iss1.1997

Awal, H., & Gusman, A. P. (2023, Februari 1). Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan *Snort* dan Iptables Berbasis *LINUX*. *Jurnal Sains dan Informatika Terapan, 2*(2), 74-80. doi:https://doi.org/10.62357/jsit.v2i1.184

Hadi, R., Abdullah, R. K., & Fitrian, H. P. (2026, Maret 26). Penerapan *Firewall* dan *Intrusion Detection System* pada Jaringan Komputer. *Journal of Computer Science and Information Technology, 2*(1), 9-15. doi:https://doi.org/10.70716/jocsit.v2i1.411

Prasetyo, F. H. (2025). Penerapan Metode *Network Development Life Cycle (NDLC)* dalam Pengembangan Jaringan Komputer. *Journal of Informatics and Communication Technology (JICT), 7*(1), 80-87. Tratto da https://ejournal.akademitelkom.ac.id/j_ict/index.php/j_ict/article/view/410

Prisscilya, V., & Santoso, T. (2022). Implementasi Keamanan Jaringan Menggunakan *Intrusion Detection System (IDS)* pada PT Mega Esa Farm. *Journal of Information Technology, 6*(1), 25-32. doi:https://doi.org/10.31284/j.integer.2021.v6i1.1205

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023, September 1). Implementasi *Intrusion Detection System*(*Ids*) *Snort* Sebagai Sistem Keamanan menggunakan Whatsapp dan Telegram Sebagai Media Notifikasi. *Jurnal Ilmiah Teknologi Informasi dan Komunikasi(JTIK), 14*(2), 358. doi:https://doi.org/10.51903/jtikp.v14i2.726

Riyanto, D. (2022). Analisis dan Perancangan Keamanan Jaringan Menggunakan *Firewall* pada Dinas Perpustakaan dan Kearsipan Provinsi Bengkulu. *Jurnal Komputer, Informasi dan Teknologi (JKOMITEK), 1*(2), 230-238. doi:https://doi.org/10.53697/jkomitek.v1i2.280

Santi, N., & Mulyanto, Y. (2024). Analisis Kelayakan Jaringan Komputer Menggunakan Alat Sniffing dan *Intrusion Detection System (IDS)*. *JATI (Jurnal Mahasiswa Teknik Informatika), 8*(4). doi:https://doi.org/10.36040/jati.v8i4.10079

Sari, S. S., & Tedyyana, A. (2024). Analisis Efektivitas Rule *Snort* dalam Mendeteksi Serangan Jaringan. *Publikasi Teknik Informatika dan Jaringan, 2*(4), 01-15. doi:https://doi.org/10.62951/repeater.v2i4.194

Setiadi, A. (2022). Manajemen Pada Jaringan *Mikrotik* Menggunakan Metode Hierarchical Token Bucket (HTB) Dan Keamanan *Firewall Intrusion Detection System (IDS)*. *Jurnal Jarkom, 9*(1), 1-9. Tratto da https://ejournal.akprind.ac.id/index.php/jarkom/article/view/3669

Setiawan, D. (2023). Implementasi Sistem Keamanan Jaringan Menggunakan Rule Based *IDS* Pada Pt Netkrida Tuah Cakrawala. *JOISIE Journal of Information Systems and Informatics Engineering, 7*(2), 381-389. doi:https://doi.org/10.35145/joisie.v7i2.4014

Tarina, C., Ismara, N., Mahara, L., Alysa, & Azimah, N. (2026, Januari 2). Perkembangan Teknologi *Firewall* Dan Strategi Pertahanan Jaringan Pada Sistem Komputer. *Jurnal Ilmu Komputer, 2*(1). doi:https://doi.org/10.62671/jikum.v2i1.154

Wijaya, F. I. (2025). Analisa Penerapan Fitur *Firewall* pada *Mikrotik* untuk Mengamankan dari Serangan Denial of Service (DoS). *Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan, 5*(3), 570-592. doi:https://doi.org/10.36312/panthera.v5i3.546

Yulianto, R., & Aprilyani, F. (2022). Sistem Keamanan Jaringan Komputer Menggunakan Metode *NDLC* Dengan *Linux* Zentyal Pada Instansi KEMENKO Maritim. *Jurnal Teknik Informatika STMIK Antar Bangsa, 6*(2), 79-86. doi:https://doi.org/10.51998/jti.v6i2.336