BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut:

1. **Aplikasi Semont** efektif mengintersepsi seluruh lalu lintas web secara *real-time* dan terdiri dari modul-modul yang bekerja sinergis untuk deteksi dan pencegahan. Ini menjawab permasalahan mengenai bagaimana merancang dan mengimplementasikan sistem IDPS yang dibutuhkan.
2. **Efektivitas Semont dalam mendeteksi dan mencegah serangan siber** telah terbukti sangat tinggi. Melalui pengujian komparatif, website SMAN 1 Rancaekek yang sebelumnya rentan terhadap injection attacks, scanning tools, brute force, serta web defacement dan webshell, Semont berhasil secara efektif mendeteksi dan memblokir serangan-serangan tersebut. Hal ini secara langsung mengatasi permasalahan kerentanan website dan ketiadaan sistem pertahanan proaktif.
3. **Fungsionalitas pemantauan lalu lintas dan respon otomatis Semont berjalan optimal.** Sistem mampu mencatat detail serangan secara komprehensif, mengirim notifikasi *real-time* ke Telegram administrator, serta melakukan pemblokiran IP dan *redirection* yang efektif. Fitur remediasi langsung untuk *web defacement* juga memberikan kontrol cepat, menjawab permasalahan bagaimana sistem dapat memantau dan menanggulangi insiden.

4. **Kelebihan penelitian ini** terletak pada implementasi sistem IDPS berbasis *signature* yang ringan dan efisien, menghasilkan *overhead* minimal pada *web server* sehingga tidak mengganggu operasional website. Pendekatan komparatif (sebelum vs. sesudah implementasi) secara empiris membuktikan peningkatan postur keamanan website secara signifikan. Selain itu, sistem ini menyediakan antarmuka pengguna yang intuitif dan notifikasi *real-time* yang sangat membantu tim IT sekolah.

5. **Kekurangan penelitian ini** adalah keterbatasan metode *signature-based* yang tidak efektif dalam mendeteksi serangan *zero-day* atau varian serangan baru yang belum terdaftar dalam basis data *signature*. Selain itu, ruang lingkup penelitian ini tidak mencakup pengembangan metode deteksi anomali berbasis statistik atau *rule-based* secara mendalam, serta tidak membahas keamanan infrastruktur jaringan secara keseluruhan di luar cakupan aplikasi web.

5.2 Saran

Berdasarkan hasil penelitian dan identifikasi kelemahan sistem, berikut adalah beberapa saran untuk pengembangan lebih lanjut dan penelitian di masa mendatang:

1. **Solusi untuk Kelemahan Sistem (Aspek Sistem):**

   a. **Pembaruan *Signature* Otomatis**: Mengembangkan mekanisme untuk memperbarui basis data *signature* Semont secara otomatis dari sumber *feed* ancaman siber terpercaya. Ini akan meningkatkan kemampuan sistem dalam mendeteksi serangan terbaru dan mengurangi ketergantungan pada pembaruan manual.

b. **Integrasi Deteksi Anomali**: Menambahkan modul deteksi berbasis anomali (misalnya, menggunakan algoritma *machine learning* untuk menganalisis pola lalu lintas abnormal) sebagai pelengkap metode *signature-based*. Ini akan memungkinkan Semont untuk mengidentifikasi ancaman yang tidak memiliki *signature* dikenal, termasuk serangan *zero-day*.

c. **Peningkatan Visualisasi Data**: Mengembangkan fitur visualisasi data yang lebih canggih pada *dashboard* SEMONT, seperti grafik interaktif untuk *trend* serangan, filter data *log* yang lebih fleksibel, dan kemampuan *drill-down* untuk analisis insiden yang lebih mendalam.

2. Saran dari Aspek Manajerial:

a. Pelatihan dan Peningkatan Kesadaran: Mengadakan pelatihan rutin bagi tim IT dan staf SMAN 1 Rancaekek mengenai pentingnya keamanan siber, cara kerja SEMONT, dan langkah-langkah respons insiden. Peningkatan kesadaran ini akan memaksimalkan efektivitas Semont dalam menjaga keamanan.

b. Kebijakan Keamanan Informasi: Mengembangkan dan menerapkan kebijakan keamanan informasi yang komprehensif di sekolah, yang mencakup penggunaan Semont sebagai bagian integral dari strategi pertahanan siber, serta prosedur standar operasional (SOP) untuk penanganan insiden.

c. Audit Keamanan Berkala: Mendorong dilakukannya audit keamanan eksternal secara berkala untuk mengidentifikasi potensi kerentanan baru dan memastikan Semont serta infrastruktur keamanan lainnya berfungsi optimal.

3. **Saran untuk Penelitian Selanjutnya**:

    1. **Pengujian Skalabilitas dan Stabilitas Jangka Panjang**: Melakukan pengujian lebih lanjut untuk mengevaluasi skalabilitas Semont dalam menangani volume lalu lintas yang jauh lebih tinggi dan kemampuannya untuk beroperasi secara stabil dalam jangka waktu yang panjang di lingkungan produksi yang lebih kompleks.

    2. **Studi Perbandingan Metode Deteksi**: Melakukan penelitian komparatif yang lebih mendalam antara metode *signature-based* Semont dengan metode deteksi anomali atau *rule-based* untuk mengidentifikasi kombinasi terbaik dalam mendeteksi berbagai jenis ancaman siber.

    3. **Pengembangan Fitur Pencegahan Lanjutan**: Menjajaki pengembangan fitur pencegahan yang lebih canggih, seperti integrasi dengan *firewall* jaringan untuk pemblokiran di lapisan yang lebih rendah, atau kemampuan untuk secara otomatis mengisolasi sistem yang terinfeksi.