BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan Penelitian dan pengujian yang dilakukan penulis dapat disimpulkan sebagai berikut :

1. Penerapan *IDS Snort* pada server web terbukti mampu mendeteksi semua jenis serangan yang diuji.

   Penerapan *IDS Snort* yang dilakukan pada server virtual ini mampu mendeteksi jenis serangan seperti *Port scanning* dan *DoS*, dari pengujian yang dilakukan *Snort* menunjukan kemampuannya dalam mendeteksi dengan cepat engan waktu deteksi *Snort* sebesar 72–989 ms pada serangan *Port scanning* dan 101–997 ms pada serangan *DoS*. Hal ini menunjukkan bahwa konfigurasi *Snort* dan aturan yang digunakan berfungsi dengan efisien dan responsif.

2. Integrasi *Snort* dengan *WhatsApp Bot* dan otomatisasi *Firewall* memberikan waktu respons yang cepat dan stabil

   .*Bot WhatsApp* yang dikembangkan mampu memproses *Alert Snort* dengan waktu sekitar 1030–1494 ms pada serangan *Port scanning* dan 1036–1884 ms pada serangan *DoS*, yang lebih tinggi karena jumlah *Alert* jauh lebih banyak. Sementara itu, waktu eksekusi *Firewall UFW* berada pada rentang 98–505 ms untuk *Port scanning* dan 291–1913 ms untuk skenario *DoS* yang memiliki beban lebih besar. Kemudian pada Gabungan waktu deteksi + pemrosesan *Bot* + eksekusi *Firewall* menghasilkan total waktu respons sekitar 1,2–2,1 detik pada *Port scanning* dan 1,6–4,2 detik pada *DoS*.

Untuk memberikan gambaran yang menyeluruh mengenai kinerja, berikut ini adalah tabel yang menyajikan rata-rata hasil dari 20 kali percobaan untuk setiap jenis serangan yang telah dilakukan.

3. Sistem keamanan yang mengintegrasikan IDS Snort dan Firewall (UFW) terbukti sangat efektif dalam mendeteksi dan mencegah serangan secara *real-time*. Efektivitas ini dapat dilihat dari dua aspek utama:
    1) Kecepatan Deteksi dan Respon:

       Port scanning : Sistem mampu menyelesaikan seluruh proses (deteksi, pemrosesan bot, hingga eksekusi blokir oleh firewall) dalam waktu rata-rata 1.615 ms (sekitar 1,6 detik).Kecepatan deteksi Snort sendiri sangat responsif, yakni hanya 448 ms.

       DoS (Denial of Service) : Meskipun beban serangan lebih berat, sistem tetap mampu melakukan pemblokiran total dalam waktu 2.700 ms (2,7 detik).Kecepatan eksekusi firewall dalam memutus koneksi penyerang rata-rata berada di angka 850 ms untuk serangan jenis ini.
    2) Otomatisasi Pencegahan (IPS):

       Sistem tidak hanya berfungsi sebagai alat pemantau (IDS), tetapi telah berhasil ditingkatkan menjadi sistem pencegahan (IPS) melalui otomatis Firewall.

    Penggunaan Bot WhatsApp sebagai jembatan eksekusi memungkinkan administrator menerima notifikasi sekaligus memastikan penyerang langsung terblokir tanpa perlu campur tangan manual pada server terminal.

Dari keseluruhan, sistem yang dikembangkan berhasil mendeteksi dan melakukan respons menggunakan *Bot* dengan Tingkat keberhasilan 100% dalam 20 kali percobaan serangan. total waktu respons di bawah 4 detik, bahkan mayoritas 3 detik

5.2 Saran

Berdasarkan saran yang dapat dikembangkan dikemudian hari dari penelitian ini adalah sebagai berikut :

1. Penelitian ini dapat dikembangkan dengan memanfaatkan machine learning untuk memperluas variasi serangan yang dapat dikenali dan pengembangan fitur *Snort* dalam mode inline.
2. Memperluas berberapa serangan yang sering menjadi target ke *web server*
3. Pembuatan Dashboard monitoring menggunakan web.

Dengan saran yang dapat diberikan, dapat berpotensi menjadi mekanisme keamanan yang handal dan cepat dalam menanggapi serangan yang mengancam ketersediaan layanan web dan *web server*.