BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian Analisis Implementasi Intrusion Detection Sistem (IDS) berbasis Snort dalam mendeteksi serangan *Brute Force* pada *SSH* berhasil mendeteksi serangan tersebut secara realtim dengan menyajikan hasil *log* serangan pada console Snort berdasarkan Custom Rules yang sudah dikonfigurasi. Sistem mampu mengenali pola serangan berulang kali dengan memanfaatkan rules yang dibuat khusus untuk mendeteksi serangaan *Brute Force*.

Kecepatan deteksi Snort menunjukkan performa yang cukup konsisten dengan *detection delay* berada di antara 1-3 detik pada sebagian besar scenario serangan yang dilakukan. Penggunaan password yang lebih komplek dapat mengakibatkan proses autentikasi pada *protocol SSH* berlangsung lebih lama sehingga menyebabkan *threshold rules* snort baru bisa terpenuhi dengan waktu yang lebih lama.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa sistem *Intrusion Detection System* (IDS) berbasis Snort memiliki efektivitas yang baik dalam mendeteksi serangan *Brute Force* pada protokol *SSH*. Berdasarkan hasil pengujian yang dilakukan, seluruh percobaan serangan yang disimulasikan berhasil terdeteksi secara konsisten oleh Snort melalui *alert* yang dihasilkan sesuai dengan *custom rules* yang telah dikonfigurasi.

Dari total enam kali percobaan serangan *Brute Force* dengan variasi kompleksitas password, Snort mampu mengidentifikasi seluruh aktivitas serangan dan mencatatnya ke dalam *log* sistem secara lengkap. Waktu deteksi yang dihasilkan berada pada rentang 1 hingga 3 detik, yang menunjukkan bahwa Snort tidak hanya mampu mendeteksi serangan secara cepat, tetapi juga efektif dalam mengidentifikasi pola serangan *Brute Force* pada layanan *SSH*.

5.2 Saran

Berdasarkan hasil penelitian Analisis Implementasi Intrusion Detection Sistem (IDS) berbasis Snort dalam Mendeteksi serangan *Brute Force SSH*, terdapat beberapa hal yang dapat dikembangkan untuk penelitian selanjutnya yaitu sebagai berikut.

1. Optimasi Rules Snort

   Dapat dilihat dari penelitian ini performa deteksi snort sangat dipengaruhi oleh rules yang dibuat. Oleh karena itu disarankan untuk melakukan pembaruan dan penyesuaian rules secara berkala

2. Implementasi *Logging* dan Visualisasi Berbasis SIEM (Security Information and Event *Management*)

   Untuk meningkatkan hasil analisis Snort dapat diintegrasikan dengan sistem berbasis SIEM seperti ELK Stack atau Splunk sehingga proses *monitoring*, visualisasi dan analisis *log* dapat dilakukan secara terstruktur dan informatif.

3. Integrasi Snort dengan Sistem Mitigasi Otomatis

   Agar hasil deteksi bisa langsung dilakukan tindakan pencegahan disarankan Snort dapat diintegrasikan dengan sistem mitigasi seperti fail2ban atau Intrusion Prevention Sistem (IPS).

4. Skenario Multiple *Attacker*

   Skenario serangan tidak hanya dilakukan oleh satu sumber perangkat saja (Single *Attacker*), melainkan menggunakan banyak perangkat untuk melakukan serangan secara bersamaan misalnya menggunakan 20 PC *attacker* atau bahkan lebih untuk mensimulasikan Distributed *Brute Force* Attack terhadap layanan *SSH*.