BAB V
KESIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil implementasi dan pengujian sistem yang telah dilakukan, peneliti dapat menyimpulkan beberapa hal sebagai berikut:

1. Berdasarkan hasil penelitian, proses integrasi sistem keamanan server berbasis Zeek dan IPTables yang terintegrasi dengan Zabbix serta dilengkapi notifikasi Telegram dan WhatsApp terbukti mampu memenuhi tujuan penelitian. Sistem yang dibangun mampu memonitor kondisi server secara cepat, tepat dan konsisten.
2. Implementasi dan evaluasi kinerja Zeek dan IPTables menunjukkan bahwa sistem mampu mendeteksi serta memitigasi seluruh jenis serangan yang diuji, meliputi ICMP *Flood*, UDP *Flood*, SYN *Flood*, *Ping of Death*, *Port Scanning*, SQL *Injection*, XSS *Attack*, *Brute Force*, dan ARP *Spoofing*. Hasil pengujian menegaskan bahwa setiap rule yang diterapkan pada Zeek dan IPTables memiliki tingkat akurasi yang tinggi, karena hanya memicu deteksi dan pencegahan terhadap jenis serangan yang benar-benar dikirimkan tanpa menghasilkan *false positive* terhadap serangan lain. Pada kategori serangan DoS, sistem terbukti mampu melakukan pencegahan secara cepat dan tepat dengan tingkat keberhasilan yang tinggi dalam menahan serangan *flooding*, sedangkan pada kategori Non-DoS mitigasi tercapai secara penuh dengan hasil yang stabil. Selain itu, penggunaan CPU, RAM, dan bandwidth tetap berada pada batas aman sehingga mekanisme deteksi dan mitigasi tidak membebani kinerja server secara signifikan.
3. Dari sisi kinerja sistem dan notifikasi, terbukti berhasil dan responsif dalam mengirimkan log ke Zabbix dan pesan peringatan ke Telegram dan WhatsApp secara cepat, tepat dan konsisten. Hasil integrasi dengan Zabbix juga mengonfirmasi tingkat akurasi monitoring, di mana grafik CPU, RAM, dan *bandwidth* yang ditampilkan sesuai dengan aktivitas serangan

yang berlangsung. Aktivasi trigger Zeek terpantau tepat waktu, dan diagram jumlah serangan yang ditampilkan pada *dashboard* monitoring konsisten dengan data hasil pengujian.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, penulis menyampaikan beberapa saran yang diharapkan dapat menjadi acuan untuk pengembangan sistem lebih lanjut serta sebagai referensi bagi peneliti selanjutnya:

1. Penelitian ini dapat dijadikan referensi bagi penelitian selanjutnya yang mengkaji topik serupa, baik dalam aspek integrasi, implementasi, maupun evaluasi sistem deteksi dan mitigasi serangan siber berbasis Zeek, IPTables, dan Zabbix.
2. Memperbanyak variasi jenis serangan pada pengujian untuk pengembangan penelitian selanjutnya, disarankan untuk menambahkan lebih banyak variasi jenis serangan siber, baik dalam kategori DoS maupun non-DoS, sehingga hasil evaluasi kinerja sistem dapat memberikan gambaran yang lebih komprehensif terhadap kemampuan deteksi dan mitigasi.
3. Penelitian berikutnya dapat dikembangkan sistem tanpa VirtualBox sebagai server menggunakan infrastruktur fisik atau layanan berbasis cloud, sehingga dapat memberikan hasil pengujian yang lebih mendekati kondisi nyata pada jaringan produksi dan meningkatkan keandalan sistem.
4. Disarankan untuk menambahkan tahapan manajemen keamanan, seperti perencanaan kebijakan keamanan, *monitoring* berkelanjutan, dan pelaporan insiden, agar penelitian memiliki cakupan yang lebih luas dan dapat diimplementasikan pada skala yang lebih besar.
5. Pada pengujian di IP publik, penelitian selanjutnya dapat menggunakan tool yang memiliki dukungan untuk lebih banyak jenis serangan, sehingga proses pengujian menjadi lebih optimal dan hasilnya lebih representatif.