BAB V PENUTUP

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilaksanakan pada PT XYZ dengan pendekatan digital forensik terhadap pencatatan log serangan di lingkungan *Apache* secara terintegrasi dengan *ELK Stack (Kibana SILK)* dan *Grafana*, dapat diambil beberapa kesimpulan terkait efektivitas alat monitoring keamanan dan analisis digital forensik yang diimplementasikan untuk mendeteksi serta merespons serangan *SQL Injection*:

Pertama, penerapan lingkungan *sandbox* dan pengumpulan data log secara terstruktur memungkinkan analisis karakteristik jejak digital *SQL Injection* pada *website* PT XYZ dapat dilakukan secara optimal. Berdasarkan hasil *monitoring log* selama periode Januari hingga April 2025, ditemukan sebanyak 243 percobaan serangan *SQL Injection* yang terdeteksi pada aplikasi *web* PT XYZ. Dari total serangan tersebut, lonjakan signifikan tercatat pada akhir Maret hingga April, dimana dalam satu hari puncak terpantau lebih dari 50 insiden yang berasal dari satu sumber IP. Analisis log juga mengidentifikasi 20 alamat IP unik sebagai pelaku serangan, di mana satu IP bertanggung jawab atas 30% dari keseluruhan aktivitas. *Payload* yang paling sering muncul adalah `'UNION SELECT'` (112 kali), `'OR '1'='1' --` (79 kali), dan `DROP TABLE` (52 kali). Melalui simulasi serangan dan pemantauan log yang terus-menerus, setiap aktivitas anomali tercatat jelas—mulai dari permintaan *HTTP* dengan *payload* mencurigakan, timestamp saat kejadian, hingga IP sumber serangan serta respons server. Otomasi *pipeline* dari *Apache* ke platform analitik seperti *Kibana SILK* dan *Grafana* mempercepat deteksi pola dan signature serangan. Dengan demikian, artefak log dapat menunjukkan pola, sumber, dan waktu serangan secara akurat, sehingga mendukung proses forensik dan mitigasi *SQL Injection* secara efektif.

Kedua, dalam visualisasi dan proses investigasi, ditemukan *user experience (UX)* dan fitur yang memberikan nilai lebih spesifik pada setiap tools: *Kibana SILK* sangat andal pada penjelajahan, deep search, korelasi lengkap serta timeline forensik/investigatif berbasis pencarian artefak. Di sisi lain, *Grafana* jelas unggul dalam presentasi tampilan data (grafik, *heatmap*, dan statistik interaktif), *alarm dashboard (alert)*, dan *layout dashboard* yang intuitif sehingga mempermudah highlight tren harian, evaluasi trafik berlebih, maupun *quick response* terhadap anomali melalui notifikasi otomatis. Observasi menyimpulkan bahwa perusahaan dapat memperoleh optimalisasi *monitoring log* baik dari sisi kedalaman investigasi waktu-kejadian dengan *Kibana SILK*, maupun responsivitas/server health

analytic melalui *dashboard Grafana*. Capaian digital forensik dalam analisis log di penelitian ini sudah berjalan merinci *trace and track* indikator serangan sesuai *best practice* serta layak direplikasi ataupun divariasikan untuk potensi skenario log selanjutnya.

Ketiga, tantangan utama dalam analisis forensik insiden *SQL Injection* di *website* PT XYZ adalah besarnya volume log yang bercampur dengan aktivitas rutin, serta variasi teknik serangan dan upaya penyamaran pelaku. Kondisi ini menyulitkan identifikasi serangan tanpa dukungan *filtering* yang tepat, apalagi dengan adanya *noise log*, risiko *false positive*, dan keterbatasan detail pencatatan log. Untuk mengatasinya, diterapkan arsitektur log *pipelining* terjadwal dari *Apache* ke *Kibana SILK* dan *Grafana*, dengan *filtering* khusus di *Logstash* guna memisahkan *noise* dari insiden sebenarnya. Pemanfaatan *dashboard* visualisasi memudahkan isolasi pola serangan, sementara standarisasi dan pembaruan format log memastikan seluruh artefak digital penting terekam demi mendukung investigasi yang sistematis dan efisien.

5.2. Recommendation

Berdasarkan hasil penelitian dan pengalaman implementasi *monitoring* log serta analisis serangan *SQL Injection* pada *website* PT XYZ, penulis memberikan beberapa rekomendasi sebagai berikut:

a. Optimalisasi Pemantauan dan Integrasi Sistem Log

PT XYZ disarankan mengintegrasikan penggunaan *Grafana* dan *Kibana SILK* secara komplementer; *Grafana* untuk visualisasi dan pemantauan harian, *Kibana* untuk proses investigasi mendalam. Pastikan juga pipeline log lintas perangkat terstruktur agar data serangan terekam dengan baik, tersip sistematis, dan memudahkan audit di kemudian hari.

b. Penguatan SOP Forensik dan Rencana Respons Keamanan

Disarankan agar audit dan analisis log forensik dijalankan secara berkala, tidak hanya saat insiden terjadi, namun juga dalam rangka pemeliharaan sistem keamanan. Proses ini perlu diakomodasi dalam bentuk *standard operating procedure* (SOP) yang mencakup tahapan pengumpulan bukti digital, pemeliharaan kronologi, dan pelacakan akses mencurigakan. Selain itu, perusahaan perlu memiliki response plan atau rencana tanggap insiden yang terdokumentasi dan dievaluasi secara rutin. Rencana ini sebaiknya meliputi deteksi dini melalui alat monitoring, langkah respons serta pemulihan saat insiden, pembagian tugas lintas tim, hingga pelaporan dan evaluasi setelah kejadian.