BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai implementasi sistem pemantauan keamanan jaringan menggunakan honeypot OpenCanary yang terintegrasi dengan ELK Stack di lingkungan Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA), dapat disimpulkan beberapa hal sebagai berikut:

1. Implementasi sistem pemantauan keamanan jaringan berbasis honeypot dan ELK Stack berhasil dilakukan secara efektif, melalui tahapan perancangan, pembangunan sistem, integrasi komponen, hingga monitoring secara *real-time* terhadap aktivitas jaringan.
2. Honeypot OpenCanary mampu mensimulasikan berbagai layanan umum seperti FTP, HTTP, SSH, SMTP, Telnet, MySQL, SMB, RDP, MSSQL, dan Git, serta berhasil mendeteksi dan merekam aktivitas mencurigakan dari sumber eksternal. Seluruh log aktivitas dikirim secara otomatis melalui *Filebeat* ke Logstash, diproses dan disimpan di Elasticsearch, kemudian divisualisasikan melalui Kibana dalam bentuk dashboard interaktif.
3. Monitoring selama 30 hari menghasilkan lebih dari 2 juta entri log serangan. Aktivitas serangan menunjukkan pola otomatis, konsisten setiap hari, dan cenderung meningkat pada akhir periode. Serangan utamanya menyasar layanan RDP, SSH, dan SQL Server, dengan IP sumber yang dominan berasal dari Vietnam dan Tiongkok.
4. Dashboard Kibana yang dibangun mampu menyajikan data log dalam bentuk visualisasi dinamis, seperti *line chart*, *bar chart*, *donut chart*, *data table*, hingga *threat map*. Visualisasi ini memberikan kemudahan dalam mengidentifikasi tren serangan dan menganalisis pola ancaman secara komprehensif.
5. Evaluasi sistem menunjukkan bahwa integrasi honeypot dengan ELK Stack berjalan secara stabil dan responsif, terutama setelah dilakukan penyesuaian

terhadap spesifikasi server serta penambahan fitur GeoIP pada Logstash. Sistem terbukti skalabel dan siap dikembangkan lebih lanjut untuk implementasi pada infrastruktur jaringan dengan skala yang lebih besar.

5.2 Saran

Berdasarkan hasil dan temuan dalam penelitian ini, terdapat beberapa saran yang diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

1. Pengembangan visualisasi

   Visualisasi data log menggunakan Kibana telah memberikan informasi yang komprehensif, tetapi tampilan *threat maps* yang tersedia dirasa kurang menarik secara visual dan interaktif. Oleh karena itu, disarankan untuk mempertimbangkan integrasi visualisasi tambahan melalui platform eksternal seperti *Grafana* atau *Splunk*, guna memperoleh tampilan geografis yang lebih dinamis dan mendukung analisis spasial yang lebih baik.

2. Peningkatan Sumber Daya Server

   Untuk mengoptimalkan performa sistem ELK Stack, diperlukan alokasi sumber daya VPS yang lebih besar, terutama dalam hal memori dan penyimpanan. Hal ini penting agar sistem tetap stabil dalam menghadapi beban data log yang tinggi, serta mendukung proses pencarian dan visualisasi tanpa keterlambatan.

3. Penerapan Sistem Otomatisasi

   Sistem pemantauan saat ini masih memerlukan beberapa tahapan manual dalam pengelolaan dan analisis data. Di masa mendatang, disarankan untuk mengembangkan mekanisme notifikasi otomatis menggunakan *Elastic Watcher* atau integrasi dengan platform keamanan lain serperti *Security Information and Event Management* (SIEM), guna memberikan peringatan dini terhadap aktivitas anomali secara otomatis.

4. Implementasi Berkelanjutan dan Pengujian Lanjutan

   Sistem ini telah terbukti efektif dalam lingkungan institusi, namun untuk mendapatkan gambaran yang lebih luas, diperlukan pengujian lanjutan dalam skala jaringan yang lebih besar atau lingkungan yang berbeda**.** Pengembangan juga dapat diarahkan untuk mendukung fitur korelasi log

dari berbagai sumber lainnya, seperti *firewall*, IDS/IPS, atau *endpoint security*.

5. Penerapan Kebijakan Keamanan

   Temuan dari monitoring menunjukkan pola-pola serangan yang dapat dimitigasi melalui penerapan kebijakan seperti penggunaan autentikasi dua faktor**,** pembatasan IP berdasarkan geografi**,** serta penghapusan akun default dan konfigurasi *hardening* pada sistem jaringan.