BAB V
SIMPULAN, DAN SARAN

5.1 Simpulan

Simpulan dari penelitian yang telah dilakukan menghasilkan beberapa simpulan diantaranya:

1. Arsitektur server multi-tenant yang aman dirancang dengan pendekatan hybrid, yaitu mengombinasikan virtualisasi menggunakan Proxmox dan kontainerisasi berbasis K3S. Proxmox digunakan untuk menciptakan isolasi berbasis *virtual machine* (VM), sementara K3S memberikan isolasi tambahan melalui kontainer. Selain itu, segmentasi jaringan menggunakan VXLAN diterapkan untuk meningkatkan keamanan dan mencegah serangan lateral antar tenant.
2. Berdasarkan *attack path analysis* terhadap arsitektur ini menunjukkan bahwa pendekatan *hybrid* memiliki sistem keamanan berlapis untuk mencegah penyerang mendapatkan akses ke target utama. *Attack path analysis* mengungkap bahwa untuk menembus sistem dan memengaruhi tenant lain, penyerang harus melalui minimal 7 tahap eksploitasi yang melibatkan VM, kontainer, dan jaringan, dengan sistem pengamanan berlapis, menunjukkan bahwa kombinasi virtualisasi dan kontainerisasi dapat mepertebal barimeter pengamanan sehingga untuk mendapatkan akses ke sistem utama harus menembus berbagai pengamanan yang diimplementasikan.

5.2 Saran

Meskipun penelitian ini telah mencapai tujuannya, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan lebih lanjut:

1. Pengujian pada Skala yang Lebih Besar:

   Penelitian ini dilakukan dalam skala terbatas dengan jumlah tenant dan VM yang relatif kecil. Untuk memastikan bahwa arsitektur ini dapat diterapkan pada skala yang lebih besar, disarankan untuk melakukan pengujian dengan jumlah tenant dan VM yang lebih banyak dan dijalankan di banyak data center. Hal ini akan membantu mengidentifikasi potensi bottleneck atau masalah kinerja yang mungkin muncul.

2. Integrasi dengan Teknologi Keamanan Tambahan:

Meskipun arsitektur yang dirancang sudah cukup aman, integrasi dengan teknologi keamanan tambahan seperti *Intrusion Detection System* (IDS) atau *Intrusion Prevention System* (IPS) dapat meningkatkan keamanan sistem secara keseluruhan. Teknologi ini dapat membantu mendeteksi dan mencegah serangan yang lebih canggih.

3. Pengujian Keamanan yang Lebih Mendalam:

   Penelitian ini menggunakan simulasi serangan berdasarkan kerentanan yang telah teridentifikasi. Untuk pengembangan lebih lanjut, disarankan untuk melakukan pengujian keamanan yang lebih mendalam, seperti penetration testing atau red teaming, untuk mengidentifikasi potensi kerentanan yang belum terdeteksi.

4. Dokumentasi dan Pelatihan:

   Untuk memastikan bahwa arsitektur ini dapat diadopsi dengan mudah oleh organisasi lain, disarankan untuk menyediakan dokumentasi yang lengkap dan pelatihan bagi administrator sistem. Hal ini akan membantu memastikan bahwa sistem dapat dikelola dengan baik dan keamanannya tetap terjaga.

5. Pemantauan dan *Logging* yang Lebih Baik:

   Implementasi sistem pemantauan dan logging yang lebih baik dapat membantu mendeteksi dan merespons insiden keamanan dengan lebih cepat. *Tools* seperti Prometheus, Grafana, atau ELK Stack dapat diintegrasikan untuk memantau kinerja sistem dan mendeteksi aktivitas yang mencurigakan.