BAB 5
PENUTUP

Bagian ini memuat kesimpulan dan saran terhadap Tesis. Kesimpulan dan saran disajikan secara terpisah, dengan penjelasan sebagai berikut:

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan terkait deteksi dan pengumpulan artefak digital insiden *web defacement* situs judi online di lingkungan berbasis cloud dengan menggunakan Wazuh dan Velociraptor, beberapa kesimpulan dapat diambil sebagai berikut:

a. Penerapan dan integrasi Wazuh dan Telegram serta Velociraptor dapat digunakan sebagai Solusi hemat dan praktis untuk melakukan deteksi dini dan tindak lanjut terhadap aplikasi public facing yang rentan terhadap serangan siber khususnya *web defacement* situs judi online, hal tersebut dikarenakan setiap aplikasi yang bersifat *public facing* pasti akan menjadi target serangan dari pihak yang tidak bertanggung jawab.
b. Pemodelan dan rekonstruksi serangan *web defacement* situs judi online berhasil dilakukan dengan menggunakan Framework Mitre Att&ck.
c. Wazuh dapat melakukan deteksi aktivitas *anomaly* secara *real-time* dan mengirimkan notifikasi ke Telegram Group. Berdasarkan perhitungan *Mean Time To Detect* diketahui bahwa rata-rata setiap 1 detik terdapat 1 alert yang terdeteksi oleh Wazuh.
d. Mekanisme *containment* menggunakan Velociraptor hanya berhasil dilakukan pada server AWS dan tidak berhasil pada server GCP. Velociraptor dapat digunakan untuk pengumpulan artefak, beberapa artefak dan *evidence* yang perlu dilakukan pengumpulan antara lain file artefak (*backdoor*), log sistem, log aplikasi, dan konfigurasi sistem.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan berkaitan dengan deteksi dan pengumpulan artefak digital insiden *web defacement* pada situs judi online di lingkungan berbasis *cloud* dengan menggunakan Wazuh dan Velociraptor, berikut adalah saran untuk penelitian lebih lanjut:

a. Melakukan integrasi Wazuh dengan OpenCTI untuk mendapatkan data terkait dengan *indicator of compromised* (IoC) sehingga dapat memperkaya rules wazuh dalam melakukan deteksi *anomaly* serta deteksi aktivitas *malware*.
b. Memanfaatkan Velocirpator untuk melakukan *Threat Hunting* terdapat server sebagai upaya *compromised assessment* sehingga server dapat bersih dari *file malicious*.