BAB V
SIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1 Simpulan

Dari hasil temuan penelitian dan pengembangan *game* edukasi untuk meningkatkan kesadaran keamanan siber, dapat disimpulkan beberapa poin penting sebagai berikut:

5.1.1 Dalam analisis terhadap *ransomware*, penting untuk memahami tidak hanya bagaimana *ransomware* bekerja, tetapi juga bagaimana proses pembuatannya dilakukan oleh penyerang. Dengan melakukan analisis dekompilasi, kita dapat mengidentifikasi komponen-komponen krusial dari *ransomware* serta teknik yang digunakan untuk memaksimalkan dampaknya. Hasil analisis dekompilasi terhadap *ransomware* mengungkapkan bahwa *ransomware* yang dianalisis menggunakan metode hybrid encryption, yang menggabungkan RSA untuk keamanan tinggi dalam mengenkripsi kunci sesi dan AES untuk efisiensi dalam mengenkripsi data yang lebih besar. Proses pembuatan *ransomware* dimulai dengan perencanaan dan penelitian, di mana penyerang mengumpulkan informasi tentang target, termasuk sistem operasi dan jenis file yang sering diakses. Informasi ini digunakan untuk menentukan algoritma enkripsi yang paling efektif. Selanjutnya, pengembangan kode *ransomware* dilakukan dengan inisialisasi kunci enkripsi RSA dan AES, diikuti dengan pemindaian sistem korban untuk menemukan file-file penting yang akan dienkripsi. File-file tersebut dienkripsi menggunakan AES, sementara file asli dihapus untuk memastikan data hanya dapat diakses dengan kunci dekripsi yang benar. Setelah enkripsi selesai, *ransomware* mengirimkan laporan ke server *Command and Control* (C&C) penyerang dan menampilkan pesan tebusan kepada korban melalui antarmuka GUI. *Ransomware* kemudian didistribusikan ke target melalui metode seperti *email phishing*. Dari perspektif keamanan digital, serangan *ransomware* ini secara signifikan mengganggu ketersediaan (*availability*) dan integritas data korban (*integrity*). *Ransomware* menghambat ketersediaan data dengan mengenkripsi file penting, membuat data tersebut tidak dapat diakses tanpa membayar tebusan. Selain itu, integritas data juga terganggu karena data yang dienkripsi tidak dapat digunakan dalam bentuk aslinya tanpa kunci dekripsi. Oleh

karena itu, memahami alur kerja pembuatan *ransomware* ini menekankan pentingnya tanggung jawab dalam menjaga keamanan dan integritas aset digital. Peningkatan kesadaran akan risiko yang ada dan penerapan praktik keamanan siber yang baik sangat diperlukan untuk menciptakan lingkungan digital yang lebih aman.

5.1.2 Penelitian ini mengembangkan aplikasi *RansomForge* menggunakan model *Game Development Life Cycle* (GDLC), mencakup tahapan inisiasi, pra-produksi, produksi, alpha testing, beta testing dan rilis. pengujian terhadap aplikasi *game RansomForge* menunjukkan hasil yang positif. Pada tahap alpha testing, metode *black box testing* memastikan semua fitur berfungsi dengan baik dalam skenario realistis, menunjukkan bahwa aplikasi memenuhi harapan pada tahap ini. Setelah berhasil, *game* memasuki beta testing dengan metode *one-on-one validation*. Umpan balik dari tester menghasilkan berbagai peningkatan penting, termasuk penambahan instruksi, penomoran soal, penyediaan kunci jawaban, dan perbaikan tombol. Meskipun hasil pengujian menunjukkan bahwa *RansomForge* telah melalui pengecekan yang menyeluruh, *game* ini masih memerlukan pengujian lebih lanjut sebelum dapat dikatakan layak untuk dirilis.

5.2 Implikasi

Berdasarkan penelitian yang telah dilakukan, dapat memberikan implikasi sebagai berikut:

5.2.1 Implikasi Teoritis

5.2.1.1 Hasil penelitian ini menjadi rujukan karya ilmiah dalam studi keamanan siber, khususnya terkait *hybrid encryption* dalam *ransomware*. Penelitian ini juga menekankan pentingnya analisis dekompilasi *ransomware* untuk mengidentifikasi komponen krusial *ransomware*, yang dapat menjadi dasar bagi penelitian lanjutan di bidang keamanan informasi.

5.2.1.2 Penelitian ini memperluas literatur mengenai penggunaan *Game Development Life Cycle* (GDLC) dalam menciptakan *game* edukasi, khususnya yang bertujuan untuk meningkatkan kesadaran keamanan siber. Ini memperkuat teori bahwa gamifikasi dapat menjadi metode efektif dalam pendidikan teknis.

5.2.2 Implikasi Praktis

5.2.2.1 Pengetahuan dari penelitian ini dapat langsung diaplikasikan oleh praktisi keamanan siber dalam mengembangkan strategi mitigasi *ransomware* yang lebih efektif.

5.2.2.2 *RansomForge* dapat digunakan sebagai alat pelatihan dalam institusi pendidikan dan organisasi untuk meningkatkan kesadaran akan keamanan siber.

5.3 Rekomendasi

Berdasarkan hasil penelitian ini, beberapa rekomendasi yang ditujukan kepada para pemangku kepentingan diantaranya sebagai berikut:

5.3.1.1 Praktisi keamanan siber: menggunakan hasil penelitian ini untuk memperkuat langkah-langkah keamanan terhadap *ransomware*, termasuk pengembangan dan penerapan alat deteksi serta strategi mitigasi yang lebih canggih.

5.3.1.2 Profesional keamanan informasi: memanfaatkan wawasan yang diperoleh dari penelitian ini untuk melakukan pelatihan internal yang lebih efektif, serta untuk mengembangkan kebijakan keamanan yang lebih ketat terkait enkripsi dan perlindungan data.

5.3.1.3 Pengembang *game* dan aplikasi edukasi: melanjutkan inovasi dalam menciptakan alat-alat pembelajaran interaktif yang relevan dan aplikatif dalam bidang keamanan siber. Kolaborasi dengan pakar keamanan akan memastikan bahwa konten yang dikembangkan tetap akurat dan up-to-date.