BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan mengenai *Analisis Hybrid Reverse Engineering Malware Windows Melalui Pendekatan Statis dan Dinamis Berbasis Lingkungan Isolasi FLARE VM*, dapat disimpulkan bahwa penerapan metode hybrid reverse engineering mampu mengidentifikasi struktur internal dan perilaku malware secara sistematis. Pada tahap analisis statis, struktur internal file Portable Executable (PE), import table, serta indikasi teknik penyamaran seperti packing berhasil diidentifikasi. Tahap analisis dinamis memungkinkan observasi perilaku runtime malware, termasuk aktivitas alokasi memori, komunikasi jaringan, serta teknik process injection.

Lingkungan isolasi FLARE VM mendukung proses analisis dengan menyediakan berbagai alat reverse engineering dalam satu sistem terintegrasi serta menjaga keamanan sistem host selama pengujian berlangsung. Melalui integrasi antara analisis statis dan dinamis, penelitian ini berhasil mengidentifikasi *Indicators of Compromise (IoC)* yang mencakup domain, alamat IP, registry artifacts serta fungsi-fungsi yang berkaitan dengan aktivitas malware jenis *Remote Access Trojan* seperti *AgentTesla*.

Dengan demikian, proses analisis hybrid reverse engineering berbasis FLARE VM dapat digunakan untuk mengidentifikasi dan menganalisis teknik *packing* dan *obfuscation* pada malware Windows sesuai dengan rumusan masalah penelitian.

5.2 Saran

Penelitian ini memiliki keterbatasan pada jumlah sampel malware yang dianalisis, yaitu satu sampel dari keluarga AgentTesla. Meskipun pendekatan *Hybrid Reverse Engineering* yang diterapkan mampu mengidentifikasi teknik penyamaran seperti *packing* dan *obfuscation*, serta tetap berjalan ketika malware melakukan deteksi terhadap proses analisis, ruang lingkup pengujian masih terbatas pada karakteristik satu keluarga malware. Oleh karena itu, penelitian selanjutnya disarankan untuk menguji model hybrid ini terhadap lebih banyak sampel malware dengan variasi teknik proteksi yang berbeda. Pengujian dapat mencakup malware yang menerapkan mekanisme *anti-virtual machine*, *anti-debugging* tingkat lanjut, maupun teknik deteksi otomatisasi analisis. Penggunaan berbagai keluarga malware akan memberikan gambaran yang lebih komprehensif mengenai konsistensi dan ketahanan metode hybrid dalam menghadapi teknik evasive yang lebih kompleks.

Selain itu, pengembangan analisis jaringan lanjutan menggunakan metode inspeksi paket secara mendalam (*deep packet inspection*) dapat dilakukan untuk memperluas visibilitas terhadap pola komunikasi *Command and Control* (C2) serta mekanisme eksfiltrasi data yang digunakan malware. Dengan perluasan jumlah sampel dan kompleksitas teknik yang diuji, penelitian selanjutnya diharapkan dapat memperkuat validitas model *Hybrid Reverse Engineering* dalam menganalisis malware Windows modern.