BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi di Indonesia membawa kemajuan signifikan dalam berbagai sektor, namun juga diiringi peningkatan ancaman keamanan siber yang terus berkembang setiap tahunnya. Berdasarkan *Laporan Tahunan Keamanan Siber 2024* yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), tercatat 330.527.636 aktivitas anomali siber sepanjang tahun 2024. Jenis serangan terbanyak berasal dari Mirai Botnet dengan 81.286.596 aktivitas, diikuti oleh phishing (26.771.610), ransomware (514.508), dan *Advanced Persistent Threat* (APT) sebanyak 2.487.041 aktivitas. Pola ancaman ini menunjukkan peningkatan serangan yang berorientasi pada pencurian data dan pengambilalihan sistem, baik melalui mekanisme enkripsi data seperti ransomware maupun kendali jarak jauh sebagaimana pada APT [1].

Jenis malware yang umum digunakan dalam kategori serangan siber adalah Remote Access Trojan (RAT), yang memungkinkan pelaku memperoleh akses penuh ke sistem korban untuk mengunduh, menghapus, atau menyalin data sensitif [2]. Salah satu variannya seperti *AgentTesla* banyak digunakan dalam serangan yang menargetkan pengguna Windows karena kemampuannya mencuri kredensial, merekam aktivitas pengguna, serta berkomunikasi secara tersembunyi dengan *command and control server* [3][4].

Kompleksitas ancaman tersebut mendorong perlunya strategi mitigasi yang aman dan terukur dengan upaya pendekatan analisis malware statis dan dinamis berbasis sandbox atau laboratorium virtual yang menjadi salah satu solusi efektif dalam meningkatkan ketahanan siber, terutama untuk sistem operasi Windows, pemanfaatan teknologi seperti VirtualBox memungkinkan pemisahan lingkungan pengujian dari sistem utama, sehingga proses analisis dapat dilakukan dengan aman tanpa resiko kerusakan permanen. Metode tersebut mendukung kegiatan reverse engineering yang memungkinkan peneliti memahami struktur

internal malware melalui pembongkaran kode serta pengamatan perilaku saat dijalankan [5].

Penelitian Widiyasono (2025) menegaskan bahwa teknik analisis statis dan dinamis merupakan pondasi dalam analisis malware modern, di mana analisis statis menitikberatkan pada pembacaan struktur biner, sedangkan analisis dinamis berfokus pada perilaku runtime di lingkungan terisolasi [6]. Beberapa penelitian sebelumnya menggunakan menggunakan *Cuckoo Sandbox* sebagai alat analisis dinamis dan *Ghidra* sebagai alat analisis statis. Keduanya terbukti efektif untuk deteksi perilaku dasar malware seperti modifikasi *registry* dan komunikasi jaringan. Namun, pendekatan tersebut memiliki keterbatasan dalam mendeteksi sampel malware yang telah melalui proses *packing* atau *obfuscation*, karena proses *automatic scan* seringkali gagal mengekstraksi perilaku tersembunyi secara mendalam [7].

Sebagai solusi dari keterbatasan tersebut, penelitian ini menggunakan FLARE VM (Forensic and Reverse Engineering Virtual Machine) sebagai lingkungan isolasi utama dalam analisis hybrid reverse engineering malware Windows yang dikembangkan oleh Mandiant (FireEye) dan dirancang khusus untuk kebutuhan analisis malware, forensik digital, serta incident response [8]. FLARE VM menyediakan lingkungan terintegrasi dengan berbagai alat analisis statis dan dinamis seperti IDA Free, Ghidra, x64dbg, Wireshark, PEiD, dan Process Hacker, yang memungkinkan proses analisis dilakukan secara menyeluruh dari dekompilasi kode hingga observasi perilaku runtime [9].

Pemilihan FLARE VM didasarkan pada fleksibilitas dan kelengkapannya sebagai lingkungan isolasi, di mana pengguna dapat melakukan analisis statis menggunakan *disassembler* dan *decompiler*, serta analisis dinamis melalui debugger dan pemantauan aktivitas sistem secara langsung. Integrasi berbagai alat dalam satu ekosistem membuat FLARE VM lebih efisien dibandingkan penggunaan terpisah seperti *Sandbox* dan *Ghidra* [8]. Selain itu, FLARE VM mampu mendukung analisis terhadap malware yang menggunakan teknik *obfuscation* dan *packing*, sehingga memberikan hasil yang lebih mendalam dalam

memahami perilaku berbahaya suatu sampel, penelitian ini diharapkan dapat membuktikan hybrid *reverse engineering* dalam mengidentifikasi dan memahami teknik penyamaran kode yang menjadi karakteristik utama malware modern.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah seperti diatas, maka dapat dirumuskan permasalahan yang akan dibahas yaitu tentang, Bagaimana proses analisis hybrid reverse engineering malware Windows berbasis lingkungan isolasi FLARE VM dalam mengidentifikasi serta menganalisis teknik packing dan obfuscation?

1.3 Batasan Masalah

Agar penelitian ini terarah dan tidak melebar dari fokus utama, maka batasan masalah ditetapkan sebagai berikut:

1. Penelitian hanya berfokus pada analisis malware yang berjalan pada sistem operasi Windows 10 (64-bit) sebagai lingkungan target pengujian.
2. Jenis malware yang dianalisis adalah AgentTesla RAT, yang dipilih karena merepresentasikan kategori malware Remote Access Trojan (RAT) dengan karakteristik teknik packing, obfuscation, dan enkripsi.
3. Proses pengujian dilakukan pada lingkungan virtualisasi terisolasi menggunakan VirtualBox, dengan konfigurasi host Windows 10 dan guest Windows 10 (FLARE VM) untuk menjamin keamanan sistem utama selama eksekusi malware.
4. Penelitian ini tidak membahas aspek kriptografi lanjutan atau analisis jaringan tingkat lanjut yang berada di luar ruang lingkup identifikasi perilaku dan struktur kode malware.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Mengidentifikasi struktur internal, fungsi berbahaya, serta teknik penyamaran kode seperti packing, obfuscation, dan enkripsi pada malware Windows jenis Remote Access Trojan (RAT) menggunakan metode analisis statis di lingkungan FLARE VM.
2. Menganalisis perilaku runtime malware, termasuk aktivitas berkas, registry, proses, dan komunikasi jaringan menggunakan Lingkungan isolasi FLARE VM.
3. Mengembangkan dan memvalidasi model integrasi analisis hybrid (statis dan dinamis) sebagai pendekatan yang komprehensif dalam reverse engineering malware untuk mendukung peningkatan keamanan siber pada sistem operasi Windows.

1.5 Manfaat Penelitian

1. Secara umum, penelitian ini diharapkan dapat menjadi referensi ilmiah dalam pengembangan analis keamanan dan peneliti forensik digital sebagai panduan dalam melakukan analisis malware windows khususnya teknik penyamaran secara aman, terukur menggunakan FLARE VM dan tool pendukung seperti Detect It Easy, x32dbg, Process Hacker, dan FakeNet-NG.
2. Secara teoritis, penelitian ini memberikan kontribusi terhadap pengembangan ilmu keamanan siber dan reverse engineering, khususnya pada integrasi metode analisis statis dan dinamis berbasis lingkungan isolasi sebagai solusi efektif untuk mendeteksi dan memahami perilaku malware modern.

1.6 Sistematika Penulisan

Sistematika penulisan dalam Skripsi ini terdiri dari lima bab yang saling berkaitan satu sama lain, yaitu sebagai berikut

BAB I PENDAHULUAN

Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan Skripsi.

BAB II TINJAUAN PUSTAKA

Berisi teori-teori yang mendukung penelitian, hasil studi literatur, serta penelitian terdahulu yang relevan dengan analisis malware dan lingkungan isolasi FLARE VM.

BAB III METODE PENELITIAN

Menjelaskan objek penelitian, alur penelitian, alat dan bahan yang digunakan, serta langkah-langkah analisis statis dan dinamis yang dilakukan pada sampel malware.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil penelitian yang diperoleh dari proses analisis statis dan dinamis terhadap sampel malware yang diuji. Pada bagian ini dipaparkan temuan terkait struktur internal, perilaku runtime, serta teknik penyamaran kode (packing dan obfuscation) yang digunakan oleh malware. Selain itu, disertakan pula pembahasan mendalam terhadap hasil analisis dan validasi efektivitas metode hybrid reverse engineering berbasis FLARE VM.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya. Kesimpulan disusun berdasarkan hasil analisis dan pembahasan, sedangkan saran ditujukan bagi peneliti, praktisi keamanan siber, maupun pihak lain yang tertarik pada topik analisis malware.