3. ANALISA DAN DESAIN SISTEM

Pada bab ini penulis akan membahas analisa permasalahan dan desain rancangan sistem yang digunakan dalam melakukan analisis malware dan pengumpulan sampel untuk pengerjaan skripsi

3.1 Analisa Permasalahan

Malware (malicious software) adalah jenis perangkat lunak yang memiliki kode atau perilaku yang dirancang untuk menyebabkan kerusakan, mengganggu, atau mengeksploitasi sistem komputer atau perangkat lainnya, biasanya tanpa izin atau sepengetahuan pemiliknya. Hal tersebut yang membuat malware menjadi area penelitian dalam bidang cyber security yang terus berkembang untuk deteksi dan analisis untuk mengatasi ancaman siber yang ada. PTIK juga sebagai data center dari Universitas Kristen Petra tidak luput dari segala jenis bentuk serangan yang ingin masuk kedalam sistem PTIK. Salah satu serangan dapat berupa sebuah malware yang bisa masuk secara langsung maupun tidak langsung. Dengan adanya kekhawatiran ini maka dilakukan penelitian dan analisis terhadap malware agar PTIK siap dan mempersiapkan langkah - langkah yang tepat untuk mengatasi maupun mencegah serangan malware.

3.2 Analisa Kebutuhan

Analisis malware sangat penting karena berperan kunci dalam melindungi sistem komputer, jaringan, dan data dari serangan berbahaya oleh perangkat lunak berbahaya (malware). Berikut beberapa alasan mengapa analisis malware sangat penting:

- **Pengidentifikasian Ancaman**:Analisis malware memungkinkan analis keamanan untuk mengidentifikasi jenis dan sifat malware yang ada. Hal ini membantu dalam memahami cara malware beroperasi, potensi dampaknya, dan sumber atau penyebarannya.
- **Deteksi dan Pencegahan**:Dengan memahami cara kerja malware, perusahaan dan individu dapat mengembangkan tindakan deteksi dan pencegahan yang lebih efektif. Analisis malware memungkinkan untuk menciptakan tanda-tanda atau pola yang dapat digunakan untuk mendeteksi malware sebelum dapat merusak sistem.
- **Penyelidikan Insiden**: Analisis malware menjadi penting ketika terjadi insiden keamanan atau serangan siber. Analisis ini membantu dalam mengidentifikasi penyebab insiden, jenis data yang mungkin telah dicuri, dan langkah-langkah yang harus diambil untuk memulihkan sistem.

- **Pemulihan Sistem**: Untuk memulihkan sistem yang terinfeksi oleh malware, analisis malware diperlukan untuk memahami cara malware beroperasi dan merusak sistem. Hal ini membantu dalam membersihkan malware, mengembalikan data yang terinfeksi, dan memperbaiki kerentanannya.
- **Perlindungan Data Pribadi**:Data pribadi adalah aset yang sangat berharga, analisis malware membantu dalam melindungi data sensitif dari pencurian dan eksploitasi oleh malware yang dirancang untuk mencurinya.
- **Pengembangan Keamanan Lebih Lanjut**: Analisis malware memungkinkan penelitian keamanan untuk mengidentifikasi tren dan perkembangan baru dalam ancaman siber. Informasi ini dapat digunakan untuk mengembangkan solusi keamanan yang lebih canggih dan proaktif.
- **Penelitian dan Pemahaman yang Lebih Baik**: Analisis malware membantu peneliti keamanan untuk memahami ancaman siber yang sedang berkembang dan mengembangkan strategi untuk melawannya secara lebih efektif.

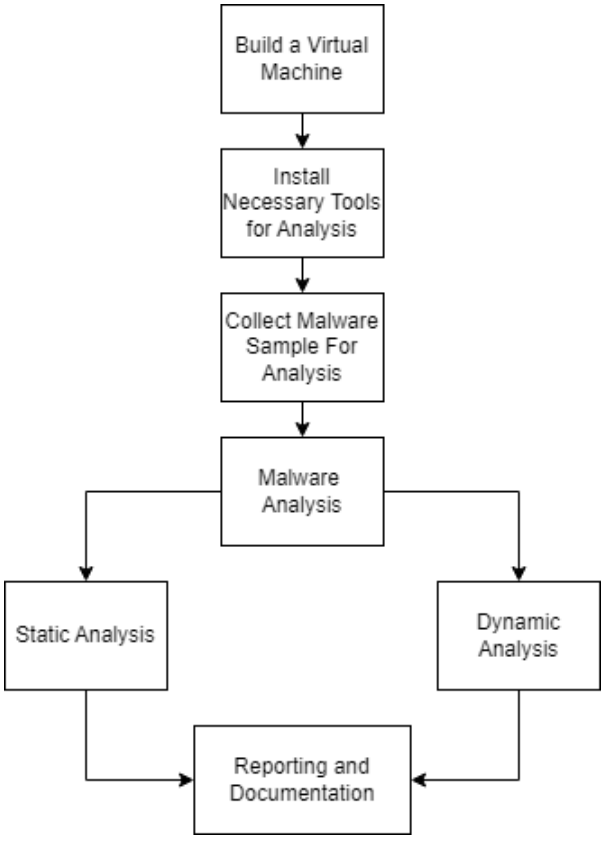
Dengan demikian, analisis malware adalah alat penting dalam melindungi sistem komputer dan jaringan dari ancaman siber yang terus berkembang. Analisis ini membantu dalam mendeteksi, mengisolasi, dan mengatasi malware, serta dalam mengembangkan solusi keamanan yang lebih kuat untuk melindungi data dan aset berharga.

3.3 Desain Sistem

Terdapat beberapa tahapan yang harus dipersiapkan sebelum melakukan analisis malware, dimulai pengumpulan sampel malware yang dikumpulkan dari situs - situs yang menyediakan sampel malware. Setiap malware yang diberikan oleh situs tersebut, harus ditinjau kembali apakah sampel yang diberikan merupakan sampel yang baru atau sampel malware yang sudah lama. Sampel malware yang dikumpulkan kemudian akan disimpan namun tidak akan diaktifkan, biasanya sampel malware menggunakan extension executable karena akan membuat malware tersebut dapat diketahui (biasanya akan menggunakan extension .file, .bat, .pdf, .pptx, .bin). Kemudian sebelum memulai proses analisis malware kita akan mempersiapkan tools - tools yang akan dibutuhkan dalam melakukan analisis, mulai dari virtual machine untuk menjadi environment tertutup agar malware tidak masuk kedalam sistem host / merusak sistem host, kemudian kita juga akan melakukan instalasi beberapa tools penting yang akan digunakan dalam melakukan analisa malware. Setelah semua tools dan environment pengujian malware sudah disiapkan kita dapat melakukan proses analisis. Proses analisis dibagi menjadi 2 bagian, yang

pertama adalah analisis secara statis dengan melakukan pembacaan dan mencari informasi terkait malware yang berada di sistem. Kemudian setelah proses analisis statis selesai akan dilakukan analisis dinamis, malware akan dijalankan pada sistem / dimasukan kedalam environment sandbox untuk dianalisis cara kerja dan kegiatan yang dilakukan oleh malware.

Setelah semua proses analisis dilakukan maka akan dilakukan proses evaluasi dari hasil analisis mulai dari berapa lama waktu yang dibutuhkan dalam melakukan malware, tools yang digunakan dalam melakukan analisis, mempelajari sifat dan karakteristik dari malware. Setelah semua proses sudah dilakukan maka akan disusun sebuah laporan yang berisi adalah jenis malware, sifat malware, tools yang digunakan dalam menganalisis malware dan bagaimana cara untuk mengatasi malware tersebut. Laporan ini yang akan menjadi data Threat Intelligence yang akan digunakan oleh PTIK dalam mengatasi dan mencegah malware.



Gambar 3.3 Grafik Analisis Malware

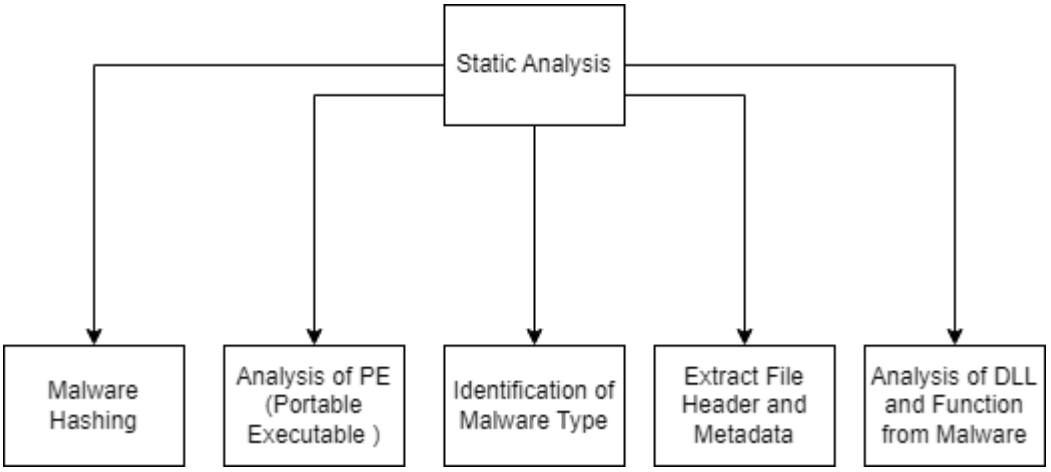
Pada Grafik 3.3 merupakan tampilan dari rencana penyusunan media analisis dan proses analisis yang akan dilakukan mulai dari membangun virtual machine, memasukan atau instalasi tools yang dibutuhkan, mengumpulkan sampel malware yang dibutuhkan sesuai kebutuhan analisa, proses analisa yang dibagi menjadi dua bagian dan untuk tahapan akhir yaitu pembuatan laporan hasil analisa

3.3.1 Proses Analisis Statis

Analisis statis malware adalah proses memeriksa dan menganalisis malware tanpa menjalankannya. Metode ini memungkinkan analis keamanan untuk memahami karakteristik malware, mengidentifikasi tindakan berbahaya yang dapat dilakukan, dan mengembangkan tindakan mitigasi yang sesuai. Berikut adalah langkah-langkah umum dalam analisis statis malware:

- **Pengumpulan Sampel Malware**: Mengumpulkan sampel malware yang akan dianalisis. Sampel ini dapat ditemukan dalam berbagai bentuk, seperti file eksekusi (misalnya, file .exe), dokumen berbahaya (misalnya, file Word atau PDF yang berisi makro berbahaya), atau kode sumber berbahaya.
- **Identifikasi Tipe File**: Tentukan tipe file dan formatnya. Ini membantu dalam pemilihan alat yang sesuai untuk analisis selanjutnya.
- **Analisis Header dan Metadata**: Periksa header dan metadata dari file. Ini mungkin mengandung informasi penting tentang sumber, versi, atau tanda tangan digital.
- **Ekstraksi String**: Identifikasi string yang mungkin berisi informasi penting, seperti alamat IP, URL, nama file, atau kata kunci yang terkait dengan tindakan berbahaya.
- **Analisis Registry dan File System**: Tinjau apakah malware mencoba mengakses atau memodifikasi registry Windows atau sistem file. Ini bisa menjadi indikasi aktivitas yang mencurigakan.

Selama seluruh proses analisis statis malware, dilakukan dalam lingkungan yang terisolasi dan aman untuk melindungi sistem Host dari potensi bahaya yang mungkin timbul dari malware tersebut.



Gambar 3.4 Grafik Analisis Malware Statis

Pada gambar 3.4 merupakan tampilan dari proses analisis statis yang akan dilakukan mulai dari mengambil value hashing dari malware, melakukan pengecekan terhadap suatu file berupa PE atau Non-PE, melakukan pengambilan jenis malware melalui hashing ID, membaca string dan function yang import oleh malware

3.3.2 Proses Analisis Dinamis

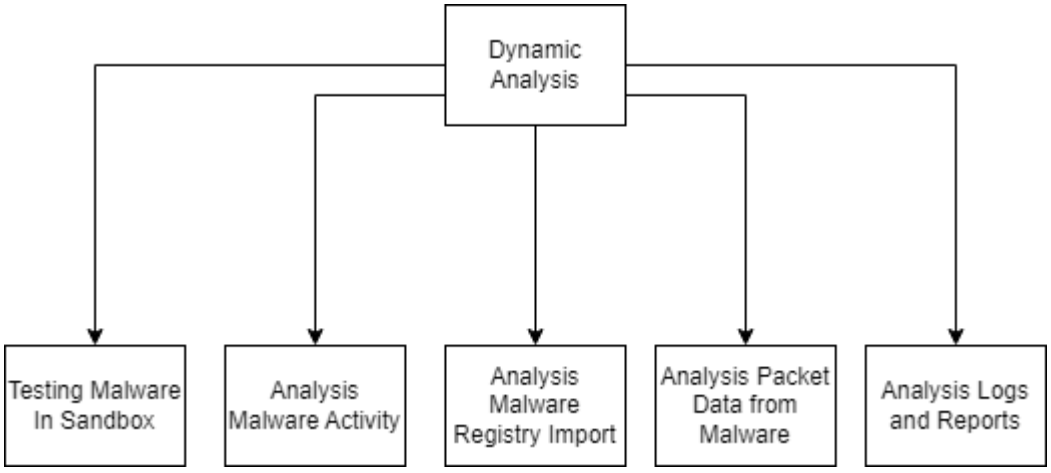
Analisis dinamis malware adalah proses memeriksa dan memahami perilaku malware dengan menjalankannya dalam lingkungan terkendali. Ini membantu analis keamanan untuk mengamati tindakan berbahaya yang dapat diambil oleh malware tanpa mengorbankan sistem produksi. Berikut adalah langkah-langkah umum dalam analisis dinamis malware:

- **Penggunaan Lingkungan Terisolasi**: Jalankan malware hanya di dalam lingkungan terisolasi atau lingkungan pasir (sandbox). Ini dapat berupa mesin virtual, lingkungan kontainer, atau alat pasir malware yang disesuaikan.
- **Pemantauan Aktivitas Jaringan** : Pantau lalu lintas jaringan yang dihasilkan oleh malware selama analisis. Catat apakah malware mencoba berkomunikasi dengan server C&C, mengunduh komponen tambahan, atau melakukan tindakan berbahaya lainnya melalui jaringan.
- **Pemantauan Aktivitas Sistem** : Amati aktivitas yang terjadi di sistem selama malware dijalankan. Ini meliputi perubahan dalam sistem file, modifikasi registry, pembuatan proses atau layanan baru, dan semua tindakan yang mencurigakan.

- **Pemantauan Proses dan Perilaku** : Perhatikan perilaku malware saat dijalankan, termasuk interaksi dengan proses sistem, percabangan, perulangan, dan tindakan berbahaya lainnya yang diambil.

- **Analisis Hasil** : Tinjau semua data yang dikumpulkan selama analisis dinamis, termasuk log jaringan, log sistem, dan hasil pemantauan. Identifikasi tindakan berbahaya yang dilakukan oleh malware.

Penting untuk menjalankan analisis dinamis dalam lingkungan yang benar-benar terisolasi untuk mencegah malware merusak sistem. Keamanan dan keselamatan data harus selalu menjadi prioritas utama selama analisis malware.



Gambar 3.5 Grafik Analisis Malware Dinamis

Pada Gambar 3.5 merupakan tampilan dari analisis yang dilakukan secara dinamis, untuk tahapan yang dilakukan mulai menguji malware pada sandbox, melakukan monitoring atas aktivitas malware, melihat pergerakan malware melalui script atau command yang dijalankan oleh malware, menganalisa packet data dan komunikasi yang dilakukan oleh malware

3.6 Proses Laporan Analisis

Pembuatan laporan analisis malware adalah langkah penting dalam proses analisis yang digunakan untuk menyampaikan temuan dan informasi secara terstruktur kepada anggota tim keamanan, manajemen, atau pihak yang berkepentingan. Ada beberapa bagian yang perlu dilampirkan pada laporan Analisis Malware sebagai berikut:

1. Pendahuluan

Jelaskan konteks analisis, termasuk bagaimana sampel malware ditemukan, tujuan analisis, dan perangkat atau lingkungan yang digunakan untuk analisis.

2. Karakterisasi Sampel Malware

Berikan informasi tentang tipe file, format, dan metadata dari sampel malware yang Anda analisis. Ini mencakup tanda tangan digital, tanggal pembuatan, atau informasi lain yang relevan.

3. Analisis Statis

Kesimpulan dari hasil analisis statis yang dilakukan pada malware

4. Analisis Dinamis

Kesimpulan dari hasil analisis dinamis yang dijalankan dan di monitor terhadap malware

5. Tindakan Mitigasi

Sarankan tindakan mitigasi yang diperlukan untuk melindungi sistem dan jaringan dari malware ini. Ini mungkin termasuk pemutakhiran perangkat lunak, pengaturan firewall, atau tindakan lain yang relevan.

6. Kesimpulan

Buat kesimpulan singkat yang merangkum temuan analisis dan tindakan mitigasi yang diperlukan.

7. Rekomendasi

Jika diinginkan, berikan rekomendasi tambahan untuk perbaikan keamanan atau langkah-langkah lanjutan yang dapat diambil.

8. Penyusunan dan Peninjauan

Pastikan untuk menyusun laporan dengan rapi dan secara sistematis. Setelah selesai, tinjau laporan untuk memastikan semua informasi relevan telah disertakan dan bahasa yang digunakan jelas.