BAB I PENDAHULUAN

I.1 Latar Belakang

Malicious software atau *malware* adalah sebuah program yang dirancang khusus untuk melakukan sebuah aktivitas yang dapat membahayakan *software* pada perangkat korban seperti *trojan, ransomware, dan downloader* (Kramer, 2010). *Trojan, ransomware* dan *downloader* adalah jenis *malware* yang paling sering menyebar, memiliki tingkat ancaman yang tinggi dan paling banyak menimbulkan masalah pada sistem komputer (Siddiqui, 2008).

Untuk mengetahui apa yang dilakukan oleh *malware*, dibutuhkan analisis untuk mengetahui aktivitas apa saja yang dilakukan oleh *malware* dan fungsi apa saja yang digunakan pada sistem setelah *malware* tersebut dieksekusi. Salah satu analisis yang akan dibahas sebagai pendukung pendukung untuk mengenali karakteristik antivirus adalah metode analisis dinamis. Analisis dinamis dilakukan dengan menjalankan sampel *malware* pada sebuah *environment* yang terkontrol dan ter *monitor* selama proses analisis (Manoppo, et al., 2020). Tindakan preventif juga berperan penting dalam mengurangi aktivitas serangan *malware* yang menginfeksi sistem komputer, salah satunya adalah dengan memanfaatkan program antivirus pada perangkat komputer.

Software antivirus adalah program yang dirancang untuk mencegah, mendeteksi, dan menghapus infeksi *malware* pada perangkat komputasi individu (Rosencrance, 2017). Antivirus disebut juga sebagai *software* perlindungan dari serangan *malware*, program ini dapat melindungi perangkat menggunakan beberapa fitur yang dimilikinya, salah satunya fitur yang terdapat pada beberapa antivirus yang memungkinkan pengguna untuk memindai perangkat penyimpanan sekunder, seperti *flash drive, hard drive* eksternal, atau kartu *memory*, untuk mencari tahu apakah terdapat *malware* yang menyebar melalui perangkat tersebut sekaligus membersihkan *malware* yang bersarang di dalamnya.

Pada penelitian ini, metode analisis dinamis digunakan sebagai data pendukung untuk mengenali karakteristik antivirus dengan cara menjalankannya dan memonitor aktivitas yang terjadi. Metode ini biasanya digunakan untuk

mengidentifikasi tindakan yang dilakukan oleh *malware* ketika dijalankan. Jumlah aktivitas *malware* akan digunakan untuk mengetahui karakteristik antivirus pada fitur yang akan diuji. Karakteristik antivirus sangat penting untuk diperhatikan. Hal ini dikarenakan jika antivirus memiliki performa yang buruk, menyebabkan kinerja sistem komputer menjadi terhambat dan berpotensi rawan untuk disusupi oleh *malware*. Selain itu, tingkat deteksi antivirus juga menjadi hal utama dalam melindungi perangkat dari serangan *malware*.

I.2 Perumusan Masalah

Merujuk kepada latar belakang yang telah dijelaskan sebelumnya, pada penelitian ini dapat diambil rumusan masalah yang mendasari penelitian ini yaitu:

a. Bagaimana mengenali karakteristik antivirus berdasarkan metrik pendeteksian *malware?*
b. Bagaimana membandingkan karakteristik dari berbagai antivirus dalam mendeteksi *malware?*
c. Bagaimana mengetahui tingkat deteksi antivirus dalam menangani *malware*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan sebelumnya, dapat ditentukan tujuan pada penelitian ini, yaitu:

a. Mengetahui karakteristik antivirus berdasarkan metrik pendeteksian *malware* menggunakan analisis dinamis
b. Mengetahui hasil perbandingan karakteristik antivirus dalam mendeteksi *malware* berdasarkan sumber daya komputasi dan waktu *scan*
c. Mengetahui tingkat deteksi antivirus dalam menangani *malware* berdasarkan akurasinya.

I.4 Batasan Penelitian

Adapun pembatasan penelitian yang dikaji dalam penelitian ini adalah sebagai berikut:

1. Analisis *malware* hanya melakukan pengambilan data dari total metrik pendeteksian *malware* sebagai pendukung untuk mengenali karakteristik antivirus.
2. Analisis karakteristik antivirus hanya menggunakan metrik penggunaan sumber daya komputasi, tidak membahas metrik lain selain metrik tersebut.
3. Sampel antivirus yang digunakan berjumlah 5 dan sampel *malware* berjumlah 6, *malware* yang digunakan hanya berjenis *trojan, ransomware dan downloader* yang berekstensi *.exe.*

I.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dapat dirasakan setelah melakukan penelitian ini dari segi teoritis dan praktis adalah sebagai berikut:

1. Keilmuan

   Penelitian ini diharapkan dapat menjadi acuan dalam memahami cara kerja *software* antivirus dan bagaimana antivirus dapat digunakan untuk mendeteksi dan mencegah *malware*. Penelitian ini juga diharapkan dapat mengidentifikasi sumber daya komputasi yang berperan penting pada antivirus dalam mendeteksi *malware* serta menambah wawasan tentang bagaimana sumber daya sistem dipengaruhi proses kerja *software* antivirus.
2. Praktis

   Secara praktis, penelitian ini diharapkan dapat dijadikan panduan dalam mengidentifikasi dan mengevaluasi karakteristik antivirus yang efektif dalam menangani *malware*, membantu dalam mengevaluasi kinerja dari antivirus yang diujikan dalam menangani *malware*. Selain itu, penelitian ini juga diharapkan dapat mengenali karakteristik penggunaan sumber daya antivirus ketika melakukan *scanning* hingga *malware* dikarantina dan kemampuan tingkat deteksi tiap antivirus.