BAB I
PENDAHULUAN

1.1 Latar Belakang

Pesatnya penyebaran *internet* menciptakan kejahatan kini tak hanya terjadi di dunia nyata, tetapi merambah ke dunia maya yang sering disebut sebagai *cyber crime*. Salah satu bentuk dari kejahatan ini adalah penyebaran *malware* yang begitu mudah [1]. *Malware* komputer pertama kali tercipta bersamaan dengan terciptanya komputer. Pada tahun 1949 salah seorang pencipta komputer yaitu John von Newman, yang menciptakan *Electronic Discrete Variable Automatic Computer* (EDVAC), memaparkan suatu makalahnya "*Theory and Organization of Complicated Automata*" [2].

Malware komputer pada umumnya dapat merusak *software* komputer dan tidak dapat secara langsung merusak *hardware* komputer tetapi dapat mengakibatkan kerusakan dengan cara memuat program yang memaksa over process ke perangkat tertentu. *Malware* memiliki karakteristik tertentu yang dapat diklasifikasikan dalam beberapa jenis yaitu *virus, worm, logic bomb, Trojan horse, backdoor, mobile code*, dan *multiple-threat malware* [3]. Efek negatif *malware* komputer adalah memperbanyak dirinya sendiri, yang membuat sumber daya pada komputer (seperti penggunaan memori) menjadi berkurang secara signifikan. Hampir 95% *malware* komputer berbasis sistem operasi Windows. *Malware* yang ganas akan merusak *hardware* [4]. Kehadiran *malware* pada komputer telah menjadi ancaman serius bagi pengguna komputer dan jaringan. *malware* pada komputer dapat menyebabkan kerusakan pada sistem operasi, aplikasi, dan file, serta mencuri informasi penting seperti data pribadi. Dalam beberapa kasus *malware* komputer bahkan dapat mengancam integritas dan keamanan nasional.

Banyak orang yang menyepelekan hal ini, mereka tidak tau ancaman besar dari perkembangan *malware*, dan mereka kebanyakan bahkan tidak peduli akan itu semua, selama mereka tidak merasakan hal yang aneh, mereka akan tenang. Padahal *malware* diam-diam bisa menyerang kapanpun. Banyak orang juga tidak memberikan perlindungan terhadap perangkat yang mereka miliki, entah apapun

alasannya, kalaupun ada yang menggunakan sebuah perlindungan seperti menggunakan *software antivirus* kebanyakan mereka hanya asal menggunakan atau hanya terima jadi pada saat baru membeli sebuah perangkat. Sekarang ini banyak sekali *software antivirus* yang beredar.

Pada penelitian ini akan membandingkan beberapa *software antivirus* yang akan diuji untuk menentukan seberapa efektif *software antivirus* tersebut, dan yang akan diujikan adalah versi gratis bukan versi yang berbayar atau premium. Mengapa versi gratis yang diuji, Ada alasan mengapa hanya memilih menggunakan *software antivirus* yang versi free dalam penelitian ini, karena kebanyakan user tidak akan menggunakan atau tidak akan mengeluarkan uang hanya untuk *software antivirus*, masih kurangnya kesadaran orang-orang betapa pentingnya sebuah *software antivirus* bagi keamanan perangkat mereka serta mereka terlalu mengsepelekan manfaat dari sebuah *software antivirus* bagi perangkat mereka dan akhirnya mereka yang ingin menginstal sebuah *software antivirus*-pun akan memakai yang versi free saja, contoh kasus nyatanya ada pada keluarga dan teman-teman dekat.

Salah satu cara untuk mencegah infeksi *malware* pada sistem adalah dengan menggunakan *software antivirus*. Untuk melindungi sistem dari serangan *malware*, banyak pengguna komputer mengandalkan *software antivirus*. *Software antivirus* adalah program yang dirancang untuk mencegah, mendeteksi, dan menghapus infeksi *malware* pada perangkat komputasi individu [5].

Pada penelitian ini, parameter yang digunakan untuk mengenali karakteristik *software antivirus* yaitu berupa sumber daya komputasi, waktu *scanning* dan tingkat deteksi pada beberapa *software antivirus* akan dilakukan analisis dan dibandingkan kinerjanya dengan *software antivirus* lainnya dalam mencegah infeksi *malware*. Jika *software antivirus* memiliki kinerja yang buruk, maka proses pemindaian akan berlangsung lama dan menyebabkan kinerja sistem komputer menjadi terhambat. Selain itu, tingkat deteksi *software antivirus* juga menjadi hal utama dalam melindungi perangkat dari serangan *malware*.

1.2 Rumusan Masalah

Rumusan masalah yang diangkat oleh penulis berdasarkan latar belakang

penelitian dapat dilihat ke dalam poin berikut ini :

1. Apakah *software antivirus* yang telah diuji mampu mengidentifikasi dan membersihkan *malware* yang telah menginfeksi komputer?
2. Bagaimana perbandingan kinerja setiap *software antivirus* yang diuji dalam penelitian ini?
3. *Software antivirus* manakah yang paling efektif dalam menghadapi *malware* dan mendapatkan skor paling baik diantara *software antivirus* yang lain dalam penelitian ini?

1.3 Batasan Masalah

Batasan masalah yang diangkat oleh penulis dapat dilihat ke dalam poin berikut ini :

1. Pengambilan sampel malware

   Batasan masalah pada pengambilan sampel *malware* dapat meliputi jumlah sampel *malware* yang digunakan, jenis dan karakteristik *malware* yang diambil. Pengambilan sampel *malware* dalam penelitian ini akan difokuskan kepada sample *malware* yang tertera pada Github InQuest.
2. Hardware dan Software yang digunakan

   Batasan masalah pada *hardware* dan *software* yang digunakan dapat meliputi spesifikasi komputer, sistem operasi yang digunakan, serta versi dan merek *software antivirus* yang akan diuji. Penelitian ini akan menggunakan komputer dengan spesifikasi yang sama untuk setiap *software antivirus* yang diuji, dan juga memperhatikan kinerja komputer saat melakukan pengujian, kondisi komputer harus sama saat melakukan pengujian tiap *software antivirus* agar pengujian ini adil bagi setiap *software antivirus*. Tidak lupa juga untuk pemilihan versi *software antivirus* yang akan digunakan adalah versi yang free atau gratis.
3. Kriteria pengujian

   Batasan masalah pada kriteria pengujian meliputi parameter

pengujian yang dilakukan, metode *scanning* yang digunakan juga harus dengan menggunakan *full scanning*, dan kriteria yang diuji diantaranya seperti durasi kecepatan dalam melakukan *scanning*, apakah mendeteksi dan menghapus *malware raw*, apakah mendeteksi dan menghapus *malware archive*, apakah mendeteksi dan menghapus *malware* terenkripsi, apakah mencegah mendownload *malware* dari *internet*, apakah mencegah menerima transfer file *malware*, apakah ada notifikasi pemblokiran, apakah ada *scanning* dan *log history*, apakah ada *realtime autoscanning*, apakah ada *online monitoring* perangkat, serta apakah *software antivirus* memberikan *Trial Version*.

4. Waktu pengujian

   Batasan masalah pada waktu pengujian dapat meliputi periode waktu pengujian dan frekuensi pengujian yang dilakukan. Penelitian ini akan menggunakan periode waktu pengujian yang sama untuk setiap *software antivirus* yang diuji, serta akan melakukan pengujian dengan frekuensi yang sama untuk setiap kategori pengujian.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti berdasarkan rumusan masalah dalam penelitiannya adalah :

1. Mengetahui apakah *software antivirus* yang telah diuji mampu mengidentifikasi dan membersihkan *malware* yang telah menginfeksi komputer.
2. Mengetahui perbandingan kinerja setiap *software antivirus* yang diuji dalam penelitian ini.
3. Mengetahui *software antivirus* manakah yang paling efektif dalam menghadapi *malware* dan mendapatkan skor paling baik diantara *software antivirus* yang lain dalam penelitian ini.

1.5 Manfaat Penelitian

1. Meningkatkan pemahaman tentang keamanan digital

   Penelitian ini akan memberikan pemahaman yang lebih baik tentang

efektivitas *software antivirus* dalam melindungi sistem dari serangan *malware*. Dengan pemahaman yang lebih baik, pengguna dapat mengambil tindakan yang tepat untuk melindungi diri dan sistem perangkat mereka.

2. Menjadi acuan untuk pengembangan software antivirus baru

   Hasil penelitian ini dapat menjadi acuan untuk pengembangan *software antivirus* baru yang lebih efektif dalam melindungi sistem dari serangan *malware*. Hal ini akan membantu mengurangi risiko terjadinya serangan dan kerusakan pada sistem perangkat.

3. Memberikan rekomendasi kepada pengguna

   Penelitian ini dapat memberikan rekomendasi kepada pengguna tentang *software antivirus* yang terbaik dan paling efektif dalam melindungi sistem mereka dari serangan *malware*. Hal ini akan membantu pengguna memilih *software antivirus* yang tepat untuk kebutuhan mereka.

4. Membantu industri keamanan digital

   Hasil penelitian ini dapat membantu industri keamanan digital dalam mengembangkan strategi dan teknologi yang lebih efektif dalam melindungi sistem dari serangan *malware*. Dengan demikian, industri keamanan digital dapat memberikan solusi yang lebih baik kepada pengguna.

5. Meningkatkan kualitas penelitian di bidang keamanan digital

   Penelitian ini dapat meningkatkan kualitas penelitian di bidang keamanan digital dan memberikan kontribusi yang signifikan dalam pengembangan pengetahuan di bidang tersebut. Hal ini dapat memperkaya literatur akademis dan membantu pengembangan penelitian di masa depan.

1.6 Sistematika Penulisan

Dalam penulisan skripsi ini, pembahasan yang diberikan mengenai sistem yang akan dibuat secara keseluruhan akan dibagi kedalam lima bab dengan sistematika penulisan sebagai berikut :

Bab I Pendahuluan

Bab ini berisi latar belakang penelitian, rumusan masalah yang diangkat pada penelitian ini, batasan masalah yang dihadapi dalam penelitian ini, tujuan penelitian ini dilakukan, serta manfaat yang dapat diambil dari penelitian ini.

Bab II Tinjauan Pustaka

Bab ini terdiri atas:

1. Studi Literatur

   Berisikan hasil-hasil penelitian terdahulu yang telah dipelajari serta memuat hal-hal yang dipelajari dan dikembangkan untuk kepentingan penelitian yang akan dilakukan.

2. Dasar Teori

   Berisikan pembahasan teori yang sudah dikumpulkan melalui beberapa jurnal dan artikel. Dasar teori memuat atas pembahasan tentang pengertian *malware*, pengertian *antivirus*, dan pemilihan *software antivirus* dan sampel *malware* yang akan digunakan pada penelitian ini.

Bab III Metode Penelitian

Bab ini berisikan tentang objek penelitian yang dilakukan, alur penelitian yang akan dilakukan, penjelasan berbagai macam persiapan untuk uji coba penelitian, diantaranya seperti Instalasi Oracle Virtual Machine Virtual Box Manager, Instalasi OS Windows Virtual Machine, Konfigurasi Windows Virtual Machine dan Skema Penelitian yang akan dilakukan, serta analisis kebutuhan alat dan bahan apa saja yang diperlukan nantinya untuk diimplementasikan pada penelitian ini.

Bab IV Hasil Dan Pembahasan

Bab ini berisikan tentang hasil dan pembahasan dari serangkaian proses uji coba penelitian dari semua *software antivirus* yang diuji, pada bab ini juga akan diperlihatkan hasil serta skor dari masing-masing *software antivirus* yang diujikan pada penelitian ini. Bab ini berisikan tabel-tabel dan penjelasan dari tabel-tabel tersebut.

Bab V Penutup

Bab ini berisikan kesimpulan dari serangkaian uji coba pada penelitian yang telah dilakukan terhadap semua *software antivirus* dan *malware* yang diujikan, serta berisikan jawaban dari rumusan serta tujuan penelitian yang telah dicantumkan pada bab 1. Bab ini juga berisikan saran dari penulis untuk penelitian kedepannya.