BAB I
PENDAHULUAN

1.1 Latar Belakang

Institusi yang memliki banyak pengguna internet pasti mempunyai beberapa masalah yang dihadapi oleh pengelola jaringan. Salah satunya adalah penyerangan dari orang yang memiliki niat jahat. Mereka yang melakukan itu untuk kepentingan dia sendiri seperti mengunci data *privasi* target, melakukan perusakan data atau *file*. Biasanya pelaku tersebut menyisipkan program yang telah dirancang untuk kepentingannya sendiri ke dalam suatu jaringan atau bisa juga melalui aplikasi dan *file* program itu disebut dengan istilah *Malicious Software (*malware).

Malware merupakan *software* yang dirancang untuk mengumpulkan informasi yang sensitive, kebiasaan dari *malware,* baik itu *Ransomware*, bad rabbit, dan NotPetya. Kebiasaan dari *malware* tersebut menghentikan proses pada sistem dan menahan data dengan menggunakan sistem enkripsi yang dapat membahayakan data tersebut. Penyebaran dan evolusi *malware* tersebut juga beragam, oleh karena itu diperlukan analisis lebih lanjut terhadap malware tersebut.(Pirozzi, 2017)

Untuk melakukan analisis, hal yang pertama kali dilakukan adalah membangun sebuah *Sandbox.* S*andbox* adalah sebuah mekanisme keamanan untuk memisahkan program yang sedang berjalan. Artinya, program yang terindikasi *malware* dijalankan pada sebuah *Sandbox* yang terisolasi untuk meminimalisir kerusakan yang dihasilkan oleh *malware* tersebut. Tools yang akan digunakan dalam *Sandboxing* yaitu Cuckoo Sandbox. Cuckoo *sanbox* memungkinkan proses *dynamic dynamic* analisis yang dapat dimonitor secara *real-time.*

Hasil analisis nantinya akan menjadi perbandingan cara kerja *malware* pada perangkat. Hasil ini juga ingin membuktikan adanya penelitian tentang *malware* untuk memetakan evolusi *malware.* Diharapkan adanya penelitian tentang analisis *malware* ini dapat memberikan kontribusi pada bidang keilmuan *forensics* agar dapat berguna di kemudian hari.

1.2 Rumusan Masalah

1. Bagaimana cara melakukan simulasi serangan dan analisis terhadap *Encryption malware* yang dijalankan di dalam *Cuckoo Sandbox*.
2. Bagaimana cara melakukan pemetaan evolusi pada *Ransomware* yang ada saat ini?

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas, peneliti membataskan masalah ini pada :

1. Perangkat yang diinjeksi malware adalah perangkat dengan sistem operasi windows yang dijalankan dengan virtualbox.
2. Lab *Sandbox* menggunakan *Cuckoo Sandbox.*
3. Sistem ini hanya menganalisa *process tree*

1.4 Tujuan Penelitian

1. Melakukan *dynamic analisis* terhadap *malware* yang tengah berjalan secara real-time menggunakan tools *Cuckoo Sandbox.* Dalam penelitian ini, analisis terhadap malware dilakukan dengan extendsion dari *Cuckoo Sandbox.*
2. Melakukan analisis terhadap perangkat dengan menggunakan tools Volatility.
3. Memperoleh kesimpulan dari hasil analisis malware pada Sandbox dan hasil memetakan evolusi malware.

1.5 Manfaat Penelitian

Manfaat dari adanya penelitian ini antara lain sebagai berikut:

1. Mengetahui adanya aktifitas *malware* pada perangkat yang dijalankan melalui Virtualbox.
2. Mengetahui cara kerja *malware* dari proses analisis melalui *Sandbox.*
3. Berkontribusi dalam bidang penelitian *forensics* sebagai dokumentasi dan implementasi proses di masa mendatang.

1.6 Metode Penelitian

Adapun metode penelitian yang penulis gunakan untuk melakukan penelitian ini diantaranya adalah:

a. Studi pustaka merupakan teknik mengumpulkan data dengan cara membaca dan mempelajari tentang analisis *malware, Sandbox,* forensics, dan hal-hal yang

berkaitan dengan penelitian ini, Sumber dari studi pustaka berupa buku, paper, jurnal, makalah dan refrensinya lainnya.

b. Untuk melakukan analisis terhadap program yang terindikasi *malware,* analisis harus dilakukan didalam sebuah environtment atau lingkungan yang terisolasi. Hal ini penting agar kerusakan yang dihasilkan oleh *malware* tidak menyebar ke sistem diluar environtment. Lingkungan ini yang dinamakan dengan sandbox.
c. Proses analisis dilakukan dengan menjalankan *malware analisys* Cuckoo Sandbox dan Volatility. Kedua hasil ini kemudian akan dibandingkan untuk memperoleh kesimpulan.
d. Pada tahap ini, peneliti akan melaporkan semua temuan yang didapat selama proses analisis kedalam laporan akhir.

1.7 Sistematika Penulisan

Sistematika penulisan penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bagian ini berisi tentang latar belakang, identifikasi masalah, menentukan batasan masalah yang akan dibahas, menjabarkan tujuan dan manfaat dari penelitian ini, asumsi metodologi serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada bagian ini berisi berbagai teori yang digunakan sebagai landasan untuk menyelesaikan permasalahan yang diangkat pada penelitian ini, Bahasan dalam bagian ini mengenai pembahasan teori dasar yang digunakan dalam penelitian, terkait malware dan *logging.*

BAB III METODOLOGI

pada bab ini berisi tentang objek dan jenis penelitian, data dan sumber data, teknik mengumpulkan data.

BAB IV DESAIN DAN PERANCANGAN SISTEM

Pada bab ini mengenai analisis terhadap kebutuhan sistem yang akan dibangun, dan sistem yang akan dibangun dalam penelitian ini berupa rancangan antarmuka dan alur proses.

BAB V IMPLEMENTASI DAN HASIL PENGUJIAN SISTEM

Bab ini berisi hasil implementasi dan penjelasan sesuai dengan perencanaan yang telah dibuat sebelumnya. Pengujian dilakukan untuk memastikan bahwa hasil akhir yang dibuat sesuai dengan kebutuhan dan karakteristik pengguna.

BAB VI KESIMPULAN DAN SARAN

pada bagian ini berisi kesimpulan yang menjelaskan tujuan penelitian dapat tercapai serta menjelaskan kelebihan dan kekurangan yang terdapat pada sistem yang telah dibuat. Semantara saran, berisi hal-hal yang dapat dikembangkan lagi kedepannya mengenai kekurangan yang masih terdapat pada sistem tersebut.