ABSTRAK

Malware merupakan program komputer yang dirancang khusus untuk melakukan aktifitas yang tidak diinginkan oleh pemiliknya atau mengganggu sebuah sistem komputer bahkan bisa merusaknya. Memahami *malware* beroperasi bisa dijadikan sebuah pembelajaran bagi mahasiswa yaitu untuk lebih dalam menganalisis *malware*. Permasalahannya adalah mahasiswa mungkin akan merasa takut ketika mereka akan menganalisis *malware* di laptop atau komputer mereka masing-masing karena kemungkinan *malware* akan tersebar kedalam sistem komputer atau laptop dari mahasiswa tersebut. Oleh sebab itu harus disediakannya fasilitas khusus yang digunakan untuk mahasiswa dalam mengekplorasi *malware* agar mencegah *malware* yang sedang dianalisis tidak menyerang sistem komputer kita. Fasilitas yang dibutuhkan yaitu menyerupai sebuah laboratorium yang khusus digunakan untuk eksplorasi dan pembelajaran lebih dalam mengenai *malware*.

Penelitian ini dimulai dari identifikasi masalah kemudian melakukan pengumpulan data dengan cara wawancara dan observasi ditempat penelitian. Hal pertama yang dilakukan yaitu observasi infrastruktur jaringan apa saja yang ada di tempat penelitian. Perancangan lab *malware* berdasarkan spesifikasi dari perangkat jaringan yang ada di tempat penelitian.

Hasil dari perancangan ini akan menggunakan tool analisis *malware* yaitu *cuckoo sandbox* yang dapat memberikan informasi dari hasil analisis statis dan analisis dinamis. Proses yang dilakukan oleh *cuckoo sandbox* yaitu akan membuat lingkungan yang terisolasi di dalam sebuah *virtual machine* dengan menggunakan sebuah *virtual networking* yaitu *host-only networking* dan ketika terjadi kerusakan pada *virtual machine* tidak akan berpengaruh kepada *host* dan mengatasi hal itu hanya tinggal menginstall ulang kembali *virtual machine*.

Kata Kunci : Malware, Analisis Malware, Lab Malware, Sandbox, Cuckoo Sandbox

ABSTRACT

Malware is a computer program designed specifically to perform activities that are not desired by the owner or interfere with a computer system can even damage it. Understanding operating malware can be used as a learning for students is to more deeply analyze malware. The problem is that students may be afraid when they will analyze the malware on their laptop or computer because of the possibility of malware will be spread into the computer system or laptop of the student. Therefore must provide special facilities used for students in exploring malware in order to prevent malware being analyzed does not attack our computer system. The facilities needed are like a laboratory specifically used for exploration and deeper learning about malware.

This research starts from the identification problem then do the data collecting by interview and observation in the place of research. the first thing to do is observation of any network infrastructure that is in place of research. The design of malware labs based on the specifications of the existing network devices in place of research.

The results of this design will use a malware analysis tool that is cuckoo sandbox that can provide information from the results of static analysis and dynamic analysis. The process done by cuckoo sandbox is to create an isolated environment inside a virtual machine using a virtual networking that is host-only networking and when there is damage to the virtual machine will not affect the host and overcome it just to re-install the virtual machine.

Keyword : Malware, Analisis Malware, Lab Malware, Sandbox, Cuckoo Sandbox