ABSTRAKSI

Perkembangan dunia teknologi yang semakin memudahkan para penggunanya mengakses informasi, seringkali menimbulkan dampak negatif bagi sistem keamanan. Keinginan seseorang semisal *hacker /cracker* untuk merusak atau bahkan mendapatkan informasi ilegal dari sebuah sistem, menuntut sistem keamanan untuk siap menanganinya. Keberadaan *malware, spyware, virus*, atau program lain yang berbahaya seringkali membuat seorang admin sistem kesulitan untuk sekedar menganalisa dan mendapatkan cukup informasi mengenai *file* tersebut.

Sistem ini dibuat untuk menjawab kebutuhan admin sistem dalam memonitor *malware* pada VPS. Sistem diintegrasikan dengan *honeypot* sebagai penangkap *malware* yang terinstall pada VPS, berguna untuk memberikan cukup informasi mengenai *file* berbahaya yang berhasil ditangkap oleh *honeypot*. Hasil *analysis* didapat dari integrasi dengan www.virustotal.com sebagai media analisator *file binary*.

Setelah dilakukan pengujian dan implementasi, didapatkan kesimpulan bahwa aplikasi *reporting* untuk *honeypot* berbasis *website* dapat meningkatkan keamanan pada VPS dari serangan *malware*. Selain itu, aplikasi ini juga mudah dimengerti, dipelajari, dan digunakan. Aplikasi ini memudahkan para *admin system* dalam memonitor VPS. Fitur pada aplikasi dapat di maksimalkan sebagai media *report* yang lengkap (*addressed RPC/DCE calls, attacked port, attacks offer a day, attacker country information, popular malware download, popular download location, dionaea statistik*). Aplikasi ini memberikan cukup informasi mengenai *detail malware* berdasarkan *analysis* dari beberapa *Antivirus*.

Kata kunci : *Malware, Honeypot, Report, Analysis*

ABSTRACT

The development of technology that make it easier for users to access information, sometimes have negative impact to security system. The urge of a person (hacker, cracker, etc) to retrieve private information from a system has to be anticipated by developing a security system. Malwares, spywares, virus or other dangerous software could initiate lots of problem for system administrator to handle and analyze information about those.

This system is built to answer the needs of a system administrator, to monitor the conditions of the server (VPS). This system is integrated with honeypot as a malware catcher installed in VPS, it is usefull to display various informations about the malicious file captured by honeypot. Analysis of the report is based on www.virustotal.com as a media to analyze binary files.

After thorough testing and implementation of this application, the main conclusions is this application are this web-based application for honeypot is capable to increase security level of the VPS in terms of malware attack. This application also is easy to understand, easy to learn, and easy to use. Beside that, this application allows administrator to monitor their VPS server. The feature of honeypot application can be maximized as a complete media report (addressed RPC/DCE calls, attacked port, attacks offer a day, attacker country information, popular malware download, popular download location, *dionaea* statistik). This application also provides sufficient malware details based on multiple antivirus analysis.

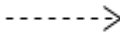
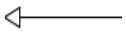
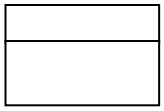
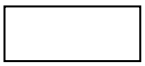
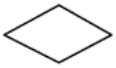
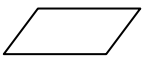
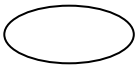
Keywords : *Malware, Dionaea, Report, Analysis*

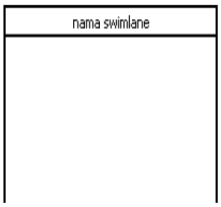
DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SIMBOL

USE CASE DIAGRAM		
NO	**SIMBOL**	**ISTILAH**
1		*Actor*
2		*Include*
3		*Extend*
4		*Association*
5		*Use Case*
CROW'S FOOT NOTATION		
6		Entitas
FLOWCHART DIAGRAM		
7		Proses / langkah
8		Titik keputusan
9		*Masukan / Keluaran*
10		Garis Alir
11		Terminasi

ACTIVITY DIAGRAM		
NO	**SIMBOL**	**ISTILAH**
12		*Actifity*
13		*Decission/* percabangan
14		*Initial Node*
15		*Actifity Final Node*
16		*Swimlane*

DAFTAR LAMPIRAN