ABSTRAK

ANALISIS KEAMANAN SERVER UNTUK BEBERAPA SERANGAN PADA JARINGAN TIC TIMOR IP

Oleh
Lilia Ervina Jeronimo Guterres
17/420702/PPA/05521

Sistem teknologi saat ini sangat berkembang pesat, dengan kemajuan internet ini, serangan pada jaringan semakin meningkat dengan terbukanya pengetahuan *hacking* dan *cracking* dengan dukungan *tools* yang tersedia dengan mudah dan mendapatkan secara gratis dapat mempermudah para *intruder* dan *attacker* melakukan aksi penyusupan atau serangan, seperti mencuri data dan informasi yang bukan hak miliknya, sehingga dapat merugikan perusahaan tersebut. Lokasi untuk melakukan pengujian pada Timor Tic IP.

Penelitian ini bertujuan untuk menyediakan suatu sistem keamanan terhadap server yang menggunakan *rules* yang dibuat untuk snort dengan fungsi memberikan pesan atau peringatan pada administrator jaringan, sehingga dengan cepat *user* mengetahui adanya serangan.

Dengan *rules* yang dibuat pada snort dapat menghasilkan deteksi serangan dan menampilkan *alert*. Pada protokol TCP memori yang terpakai 764 Mb dengan total serangan sebanyak 4099. Untuk protokol UDP *flooding* dengan memori yang terpakai sebesar 9140 Mb dengan total serangan 1310 sedangkan untuk serangan protokol ICMP *flooding* dengan total serangan 305864 dan memakan memori sebesar 5808 Mb

Kata Kunci: *Web Server Security, Snort, BASE.*

ABSTRACT

THE ANALYSIS OF SERVER SECURITY FOR MULTIPLE ATTACKS ON THE TIC TIMOR IP NETWORK

by

Lilia Ervina Jeronimo Guterres
17/420702/PPA/05521

The current technology is changing rapidly, with the significant growth of the internet technology, cyber threats are becoming challenging for IT professionals in the companies and organizations to guard their system. Especially when all the hacking tools and instructions are freely available on the Internet for beginners to learn how to hack such as stealing data and information. The location of the testing was Timor Tic IP.

This research was intended to make a security system on server using rules made for snort with function to give massage or warning to network administrator, so user can identify attack.

Rules made on snort can detect attack and display alert. In TCP protocol it used 764 Mb memory with total 4099 attacks. For UDP flooding 9140 Mb memory was used with 1310 attacks. Meanwhile for ICMP flooding protocol there were 305864 attacks and used memory of 5808 Mb.

Keywords: Web Server Security, Snort, BASE.