ABSTRAK

Teknologi *intrusion detection & prevention* merupakan teknologi pilihan bagi berbagai pihak saat ini untuk menjamin keamanan dan keabsahan informasi yang dimiliki oleh sebuah perusahaan. Perangkat *Intrusion detection & prevention* dapat digunakan untuk menggantikan perangkat keamanan lama seperti *firewall*. Perangkat *Intrusion detection & prevention* sendiri tersedia dalam berbagai jenis, dari yang berjenis perangkat lunak baik tanpa bayar(*open source*) atau bayar, hingga perangkat keras.

Perangkat *Intrusion detection & prevention* berbasis *open source* mempunyai keunggulan dalam kemudahan kustomisasinya. Kustomisasi sangat dibutuhkan karena kebutuhan pengamanan setiap perusahaan biasanya sangat berbeda-beda, sehingga penerapan perangkat ini dalam suatu IPS(*Intrusion Prevention System*) akan memerlukan perlakuan khusus sesuai dengan kebutuhan perusahaan.

Dalam penelitian ini dilakukan pengembangan perangkat lunak untuk membantu IPS yang memiliki kemudahan dalam kustomisasi tanpa mengurangi kemampuan perangkat lunak ini untuk mengenali gangguan keamanan jaringan lewat *internet*. Menganalisa masukan sebuah IP dalam jangka waktu 1 jam perangkat lunak membantu IPS dalam hal peringatan sehingga lebih baik mengenali sebuah gangguan keamanan jaringan *internet*.

Hasil yang diperoleh dari penelitian ini ialah sebuah sistem keamanan *intrusion detection & prevention* dan kebijakan yang terstruktur namun tetap adaptif sehingga mampu menghadapi gangguan kemanan jaringan lewat *internet* yang selalu berkembang. Sistem peringatan gangguan keamanan yang lebih terarah menjadi kunci yang membuat perangkat lunak ini dapat membantu pengguna dalam menentukan apakah sebuah peringatan itu harus ditanggapi serius atau tidak.

xi+53 halaman; 15 gambar; 8 tabel; 10 dokumentasi analisa studi kasus; 2 dokumentasi implementasi framework
Daftar acuan: 30(2001-2008)

ABSTRACT

Intrusion detection & prevention technology is a mechanism to guarantee security and protect information owned by a company. Intrusion detection & prevention technology has been known as a replacement for basic firewall technology. Intrusion detection & prevention technology are available software and hardware based. In software based can be as free(open source or not) or paid.

Customization in the source code is one of the strength of open source based intrusion detection & prevention technology. Customization is needed because each company may need some behaviours from the technology itself, so the implementation of this IPS(Intrusion Prevention System) will need a special modification to fit company needs.

This research will develop an addon IPS software that is easy to customize without making IPS vulnerable a network security disruption over internet. The software will analyze an input IP address from one hour IPS log so it can recognize the attack.

The result of this research is an intrusion detection & prevention security sistem and structured policies. The system itself can handle network security attack over the internet. The summarized security attack warning is the key to make sure the attack. This software will provide only the important warning to the user.

xi+53 pages; 15 figures; 8 tables; 10 study case analysis attachments; 2 framework implementantion attachment

Bibliography: 30(2001-2008)