

ABSTRAK

Nama : Mohamad Iqbal
NIM : 41517120057
Pembimbing TA : Emil R. Kaburuan, Ph.D
Judul : Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan *Siem* Pada Jaringan Komputer PT.Gloria Maju Cahaya

Keamanan informasi terlalu penting di zaman teknologi sekarang ini. Penyimpanan dan penyebaran informasi saat ini sudah tidak memakai media kertas, tapi banyak memakai teknologi komputer dan internet. Dengan berkembangnya teknologi internet dapat mempermudah pekerjaan dan juga dapat memberikan efisiensi waktu dan tempat tetapi dengan segala manfaatnya yang besar internet tidak serta merta membuat para pengguna merasa aman. di samping kemudahan akses, terdapat pula potensi serta gangguan berbahaya pada jaringan ancaman yang mengintai misalnya Jenis serangan yang terjadi pada server meliputi *port scan detection*, *brute force* dan *Denial-of-Service (DoS)*. Oleh karena itu, dibutuhkan pendeteksi dan pertahanan untuk melawan serangan terhadap jaringan untuk melindungi informasi penting dalam jaringan. Sejalan dengan perkembangan teknologi informasi, peralatan-peralatan pendukung jaringan komputer masih sangat diperlukan. Peralatan tersebut pun kini menjadi komponen penting dalam pembangunan jaringan komputer. Perkembangan teknologi keamanan jaringan saat ini sudah terdapat teknik mendeteksi serangan jaringan seperti *honeypot* dan *Siem*. *Honeypot* terdiri dari sistem pencegahan intrusi (*Interruption counteractive action framework*) yang terletak di taraf Penyedia Layanan Internet. *IPS* kemudian membentuk jaring pengaman untuk melindungi data pergerakan yg dipilih. evaluasi *honeypot* mempromosikan reproduksi luas dan gugusan data pasti diperkenalkan, yang membagikan aktivitas *honeypot* serta *overhead* yang rendah. *Honeypot* mengantisipasi agresi semacam itu serta mengurangi server. *IDS* yang berlaku umumnya dimodulasi untuk membedakan agresi sistem tingkat otoritas yang diketahui. Spontanitas ini membentuk sistem *honeypot* kuat melawan serangan pada jaringan *Security information and event management (SIEM)* akan memberikan keamanan yang mengadopsi metodologi yang dipergunakan untuk meng korelasi log, peristiwa, mengalir dari komputasi perangkat, sistem dan layanan terdistribusi dengan baseline keamanan (kegiatan pengguna serta aplikasi, kegiatan basis data dan kegiatan jaringan).

Kata kunci:

Honeypot, *Security information and event management (SIEM)*, *Denial-of-Service (DoS)* , *port scan detection*, *brute force* ,ilmu komputer, universitas mercu buana

ABSTRACT

Name : Mohamad Iqbal
Student Number : 41517120057
Counselor : Emil R. Kaburuan, Ph.D
Title : Uji Coba Sistem Keamanan Jaringan Menggunakan
Honeypot dan *Siem* Pada Jaringan Komputer
PT.Gloria Maju Cahaya

Information security is too important in today's technological age. Currently, the storage and dissemination of information does not use paper media, but uses computer and internet technology a lot. With the development of internet technology, it can make work easier and can also provide time and place efficiency, but with all its great benefits the internet does not necessarily make users feel safe. In addition to the ease of access, there is also the potential and dangerous interference on the network of threats that lurk, for example. Types of attacks that occur on servers include port scan detection, brute force and Denial-of-Service (DoS). Therefore, it takes detection and defense against attacks against the network to protect important information on the network. In line with the development of information technology, computer network support equipment is still very much needed. The equipment is now an important component in the construction of computer networks. The development of network security technology currently includes techniques for detecting network attacks such as honeypot and Siem. Honeypot consists of an intrusion prevention system (Interruption counteractive action framework) located at the Internet Service Provider level. The IPS then forms a safety net to protect the selected movement data. Honeypot evaluation promotes extensive reproduction and definite data sets are introduced, which provides honeypot activity and low overhead. Honeypot anticipates such attacks and reduces servers. The prevailing IDS is generally modulated to discriminate against known authority level system aggressions. This spontaneity establishes a robust honeypot system against attacks on the network. Security information and event management (SIEM) will provide security that adopts the methodology used to correlate logs, events, flows from computing devices, distributed systems and services with a security baseline (user and application activity, activity). database, network activity.

Keywords:

Honeypot, Security information and event management (SIEM), Denial-of-Service (DoS), port scan detection, brute force, computer science, mercu buana university