

ABSTRACT

Thesis Title : IMPLEMENTATION OF HONEYPOT WITH FWSNORT (FIRWALL SNORT) AND PSAD (PORT SCAN ATTACK DETECTOR) AS INTRUSION PREVENTION SYSTEM FOR NETWORK SECURITY AT LUBUK BASUNG HOSPITAL

Lubuk Basung Regional Hospital stores a lot of staffs and patients. Data storage requires a convincing security system considering that data contains important and private information. Lack of network security makes data thieves or what we usually call as a “hackers” are free to hack data on the target server. This research was carried out using Honeypot to maintain network security at Lubuk Basung Regional Hospital. Honeypot itself is a computer security system designed to attract hackers by providing fake targets which has a function as a distraction for hackers. Snort is an open source and concise application or software that is very useful for observing activity on a computer network. Snort can be used as a light-scale Intrusion Detection System (IDS), and this software uses a rules system that is relatively easy to learn to detect and record (logging) various types of attacks or intrusions by detecting attacks and forwarding them to the administrator so that can be stopped. The advantage of the previous method splices by the Intrusion Prevention System (IPS) method which monitors all network activity and immediately prevents interference or attacks such as blocking or dropping programs.

Keywords : Lubuk Basung Regional Hospital, Network Security, Honeypot, Snort, Intrusion Detection System, Intrusion Prevention System

ABSTRAK

Judul Skripsi : IMPLEMENTASI HONEYPOT DENGAN FWSNORT (FIRWALL SNORT) DAN PSAD (PORT SCAN ATTACK DETECTOR) SEBAGAI INTRUSION PREVENTION SYSTEM UNTUK KEAMANAN JARINGAN PADA RSUD LUBUK BASUNG

RSUD Lubuk Basung merupakan tempat dimana terdapat banyak data petugas maupun pasien. Dengan adanya data yang disimpan, tentu sangat diperlukan pengamanan pada data tersebut. Kurangnya keamanan jaringan membuat para pencuri data atau biasa kita sebut *Hacker* yang leluasa untuk melakukan *Hacking* pada suatu data yang ada pada *server* target. Penelitian ini menggunakan *Honeypot* dalam menjaga keamanan jaringan pada RSUD Lubuk Basung. *Honeypot* sendiri merupakan sebuah sistem keamanan komputer yang dirancang untuk menarik *Hacker* dengan menyediakan sasaran palsu yang terlihat menarik bagi *Hacker*. *Snort* merupakan sebuah aplikasi atau *software* yang bersifat *open source*. *Snort* adalah sebuah *software* ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan computer. *Snort* dapat digunakan sebagai *Intrusion Detection System* (IDS) yang berskala ringan (*lightweight*), dan *software* ini menggunakan *rules system* yang relatif mudah dipelajari untuk melakukan deteksi dan pencatatan (*logging*) terhadap berbagai macam serangan atau penyusupan dengan cara mendeteksi serangan dan diteruskan ke *administrator* agar dapat dihentikan. Selanjutnya metode *Intrusion Prevention System* (IPS) melakukan monitoring terhadap seluruh aktivitas jaringan dan langsung melakukan pencegahan terhadap gangguan atau serangan seperti *Blocking* atau *Drop program*.

Kata Kunci : RSUD Lubuk Basung, Keamanan Jaringan, *Honeypot*, *Snort*, *Intrusion Detection System*, *Intrusion Prevention System*