ABSTRAK

Saat ini, perkembangan teknologi semakin lama semakin pesat. Diawali dengan munculnya berbagai teknologi – teknologi di bidang ICT, khususnya pada *website/* aplikasi web yang telah banyak berkembang, baik dari segi kompplexitas maupun fungsionalitasnya. Namun perkembangan pada *website* ini juga mengakibatkan peningkatan serangan yang dilakukan oleh attacker. Sampai sekarang, 60 % dari semua serangan yang ada di internet merupakan serangan yang ditujukan pada *website*. Hal ini seiirng dengan meningkatnya pengetahuan , teknik, dan tool yang dipakai dalam melakukan penyerangan.

Honeypot merupakan suatu sistem yang sengaja dirancang untuk disusupi oleh penyusup. Hal ini dimaksudkan untuk mengelabui penyusup sehingga akan menghabiskan sumber dayanya pada sistem honeypot tersebut. Tujuan dari pembuatan honeypot ini untuk mendapatkan informasi yang akurat dari pihak penyusup. Nantinya informasi yang didapat dari honeypot akan dijadikan acuan untuk meningkatkan sistem keamanan yang telah ada, seperti *IDS Snort*.

Hasil dari tugas akhir ini adalah *Honeypot Glastopf* memiliki kemampuan dalam mengemulasikan celah – celah keamanan seperti LFI, RFI, SQL Injection (serangan yang terdeteksi 92,08%) dan memiliki kemampuan *logging* informasi – informasi serangan / penyerang yang nantinya dapat digunakan untuk meningkatkan sistem keamanan yang telah ada. Dari sisi *success rate,* performansi *Honeypot Glastopf* dapat menyamai hasil yang dimiliki server web pada pengujian dari 10 - 1.000 request dengan memiliki persentase sebesar 100%, tapi pada pengujian 10.000 request mengalami penurunan menjadi 55,93%.

Kata Kunci: *Honeypot, SQL Injection, remote file inclusion, local file inclusion, IDS, success rate*