ABSTRAK

Semakin pesat perkembangan Teknologi informasi maka semakin banyak juga cara atau trik untuk membobol sistem keamanan digital yang sangat rentan, Menurut kompas.com pada bulan maret 2020 tokopedia mengalami kebocoran data yang mempengaruhi 15 juta pengguna. Pentingnya membangun suatu sistem keamanan agar tidak disalahgunakan oleh orang yang tidak bertanggungjawab yang dapat merugikan banyak orang, Maka dibutuhkan sebuah sistem keamanan yang dapat mengamankan server dari berbagai serangan. Honeypot merupakan sebuah server palsu yang dapat menjadi solusi untuk melindungi server dari serangan hacker. Saat hacker berhasil mendapatkan akses terhadap server utama maka semua data penting dapat disalahgunakan,oleh karna itu mengalihkan server utama menjadi server buatan pada SSH,webserver dan wordpress menjadi salah satu solusi untuk melindungi server utama. Pada penelitian ini dibangun sistem honeypot menggunakan 3 buah honeypot yaitu cowrie untuk mengamankan SSH,snare untuk mengamankan webserver dan plugin untuk mengamankan wordpress metode pengamanan menggunakan *signature-based*. *Signature-based* pada dasarnya setiap aktifitas berupa serangan akan memiliki jejak/footprint tersendiri,dari footprint tersebut dilakukan analisa dan didapatkan signature dari serangan. Pengujian dilakukan dengan menampilkan hasil dari serangan yang dilakukan secara live dan dapat mengetahui datang darimana sumber serangan tersebut. Hasil pengujian mendapatkan alamat ip penyerang,waktu dan tanggal penyerangan dan tools yang digunakan.

Kata Kunci: Hacker,Honeypot,Cowrie,Snare,Wordpress