ABSTRAK

SSH merupakan layanan *secure shell* yang dapat mengamankan komunikasi *data* antar *host* dengan cara mengenkripsi *path* komunikasi *data* tersebut sehingga *transmisi data* antara *server* dan *client* dapat terlindungi dari ancaman penyerang.

Akan tetapi, layanan SSH tidak dapat mendeteksi jika terjadi serangan, karena apabila penyerang berhasil menemukan *username* dan *password* yang telah terenkripsi penyerang akan dapat mengetahui isi dari sistem komputer *target*. Pengguna atau admin juga tidak dapat mengetahui ancaman dan serangan yang dilakukan penyerang di dalam sistem komputer. Oleh karena itu, diperlukan *tools* yang dapat mendeteksi ancaman dan serangan yang dilakukan penyerang yang mencoba masuk ke dalam sistem komputer.

Kippo Honeypot merupakan *tools ssh honeypot* yang dirancang untuk membangun sistem tiruan yang dapat menjebak penyerang yang mencari celah untuk masuk ke dalam sistem asli. Kippo honeypot termasuk dalam kategori *medium-interaction* yang digunakan untuk membuat layanan tiruan yang dapat mengawasi setiap interaksi yang dilakukan penyerang, sehingga admin (pengguna) dapat mendeteksi segala aktifitas interaksi *shell* yang dilakukan penyerang. Admin dapat memantau dan mengetahui hasil serangan yang dilakukan penyerang menggunakan kippo grpah, kippo graph berguna untuk menampilakan hasil *log shell* yang penyerang lakukan untuk mencari celah agar dapat masuk ke dalam sistem komputer *target* melalui *webserver*.

Kata Kunci: Keamanan Jaringan, SSH, Kippo Honeypot, Kippo Graph.