ABSTRAK

Beberapa waktu lalu sering terjadi peretasan terhadap web oleh hacker, seperti yang terjadi pada Lembaga BPJS pada bulan Mei 2021 yang menyebabkan bocornya data pengguna sebanyak 279 Juta dan diperjual belikan dengan harga 0,15 Bitcoin atau 87,6 Juta Rupiah oleh pihak yang tidak bertanggung jawab pada forum online, oleh karena itu dibuatlah sistem yang dapat menjebak hacker ketika melakukan penyerangan terhadap web. Sistem yang dibuat disini menjebak hacker yang akan melakukan penyerangan terhadap web. Sistem akan mendeteksi penyerangan dan akan mengirimkan pemberitahuan bahwa telah terjadi sebuah serangan kepada web, sistem ini dinamakan dengan Honeypot. Honeypot yang digunakan adalah Snare dan Tanner. Snare melakukan penyalinan web yang diserang oleh hacker, ketika serangan terjadi snare akan mengirimkan informasi kepada tanner untuk disimpan, kemudian tanner akan memberikan informasi kepada administrator web bahwa telah terjadi penyerangan. Sistem dibangun pada sistem operasi ubuntu yang berjalan secara virtual menggunakan VMWare dengan menggunakan metode NDLC dan melakukan pengujian dengan menggunakan teknik penyerangan XSS, Brute Force, dan SQL Injection, dari pengujian tersebut Honeypot dapat melakukan deteksi penyerangan dalam bentuk catatan atau Log yang kemudian disimpan dan dapat ditampilkan pada antarmuka *web,* serangan XSS dideteksi dengan menggunakan emulator XSS yang disediakan oleh Honeypot begitu juga dengan Brute Force, dan SQL Injection pendeteksian dilakukan dengan menggunakan Emulator Brute Force dan SQLi oleh Honeypot.

Kata Kunci: Hacker, Honeypot, Snare dan Tanner, NDLC, Teknik Penyerangan