RINGKASAN

Imeplementasi *Intrusion Detection System* (IDS) menggunakan *Honeypot* dan *Port Knocking* berbasis Ubuntu Server, Arsya Duta Pratama, NIM E32211977, Tahun 2024, 66 hlm, Teknik Komputer, Politeknik Negeri Jember, Beni Widyawan S.T, M.T. (Dosen Pembimbing)

Beberapa aplikasi atau sistem telah dikembangkan dan dikerahkan untuk memerangi serangan yang terjadi. Misalnya teknik observasi menggunakan firewall atau *Intrusion Prevention System* (IPS) untuk mencegah serangan atau mendeteksi timbulnya serangan menggunakan *Intrusion Detection System* (IDS). Honeypot adalah sebuah sistem atau komputer yang sengaja digunakan sebagai umpan untuk menjadi sasaran penyerang. Komputer ini melayani serangan yang dilakukan oleh penyerang dengan cara menyusup ke server. Honeypot akan memberikan data palsu jika ada sesuatu yang aneh memasuki sistem atau server. Secara teori, honeypot tidak akan mencatat lalu lintas yang sah. Dengan demikian terlihat bahwa orang-orang yang berinteraksi dengan honeypot adalah semua pengguna yang menggunakan sumber daya sistem yang digunakan secara ilegal. Oleh karena itu, honeypot seolah-olah menjadi sistem yang berhasil ditembus oleh penyerang, padahal penyerang tersebut tidak menembus sistem sebenarnya melainkan sistem palsu.

Honeypot Cowrie merupakan alat keamanan jaringan yang bertindak sebagai server palsu. Ini dirancang untuk merekam upaya brute force dan interaksi shell yang dilakukan penyerang. Cowrie juga berperan sebagai proxy untuk SSH dan Telnet, memungkinkan pengamatan perilaku penyerang terhadap sistem lain. Cowrie dikembangkan dari Kippo, honeypot interaksi rendah sebelumnya. Dengan Cowrie, administrator jaringan dapat memahami lebih baik tentang metode, taktik, dan prosedur yang digunakan oleh penyerang, yang sangat membantu dalam meningkatkan keamanan jaringan.