INTISARI

ANALISIS DAN IMPLEMENTASI *HONEYPOT* TERDISTRIBUSI SEBAGAI DETEKSI AKTIVITAS *BLACKHAT* DALAM JARINGAN

Keamanan sistem komputer yang secara langsung terkoneksi ke internet menjadi semakin penting setiap harinya karena penggunaan ribuan komputer yang dikompromikan secara intensif mencari kelemahan pada sistem komputer dapat berujung pada serangan yang sukses. Agar mampu mempelajari motif, taktik, dan alat yang sekarang banyak digunakan oleh komunitas *blackhat*, sistem *honeypot* dapat dengan mudah dimanfaatkan untuk tujuan tersebut. Makalah ini memuat analisis dan implementasi beberapa sensor Dionaea yang diintegrasikan menggunakan Hpfeeds pada sistem MHN (*Modern Honey Network*) dalam jaringan internet kampus Universitas Gadjah Mada untuk menemukan aktivitas *blackhat* berupa pola dan *cluster* serangan terhadap *network services* serta *malware* sebagai informasi terhadap administrator.

Kata Kunci—*honeypot*; Dionaea; *cluster* serangan, *malware*

ABSTRACT

ANALYSIS AND IMPLEMENTATION OF DISTRIBUTED HONEYPOT AS BLACKHAT ACTIVITIES DETECTION IN THE NETWORK

Security of computer systems that are directly connected to Internet is become more important every day as the use thousands of compromised computers which intensively looking for vulnerability in computer systems can lead to successful attacks. In order to learn motives, tactics, and tools that are now widely used by the blackhat communities, honeypot system can be easily utilized for that purpose. This paper is about the analysis and implementation of several Dionaea sensors that integrated using Hpfeeds on the MHN system (Modern Honey Network) in the Universitas Gadjah Mada internet network to find blackhat activities, patterns and clusters of attacks on network services, also malwares as information to administrator.

Keywords— honeypot; Dionaea; cluster of attacks, malware