Jurnal Informatika Universitas Padjadjaran ISSN : 2503-5258
Vol. 01 No. 01 Agustus 2016

NETWORK BEHAVIOR ANOMALY DETECTION (STUDI KASUS DI GEDUNG D PUSAT PELAYANAN BASIC SCIENCE UNIVERSITAS PADJADJARAN)

Billal Hadian[1)], Erick Paulus[2)], Deni Setiana[3)]

Email : [1)]billal2001@mail.unpad.ac.id, [2)]Erick.paulus@unpad.ac.id, [3)]deni@unpad.ac.id

Program Studi Teknik Informatika, Departemen Ilmu Komputer, FMIPA Universitas Padjadjaran

ABSTRACT

Detect and understand anomalies in network activity is a topic that is promising in the field of network security. Threat or security threats can be found by studying anomalies or irregularities that occurred in the observed network. In this research will be discussed procedures anomaly detection in the activities of the network, as well as the classification and characteristics of the threat that may be the cause of the anomaly. Network activity data used in this study was obtained from direct monitoring process, which is expected to be able to represent the network activity in real circumstances. At the end of this study will be reported findings - findings that successfully obtained during the study, and its link network activity in conditions of daily operations.

Keywords — Network Behavior, Network Security, Anomaly Detection, Threat Classification

ABSTRAK

Mendeteksi dan memahami anomali dalam aktifitas jaringan merupakan topik yang menjanjikan di bidang keamanan jaringan. *Threat* atau ancaman keamanan dapat ditemukan dengan mempelajari anomali atau penyimpangan yang terjadi pada jaringan yang diamati. Dalam penelitian ini akan dibahas prosedur pendeteksian anomali dalam aktifitas jaringan, serta klasifikasi dan karakteristik dari *threat* yang mungkin menjadi penyebab anomali tersebut. Data aktifitas jaringan yang digunakan dalam penelitian ini diperoleh dari proses pemantauan secara langsung, yang diharapkan akan mampu merepresentasikan aktifitas jaringan dalam keadaan sebenarnya. Di bagian akhir penelitian ini akan dilaporkan temuan – temuan yang berhasil didapatkan selama penelitian berlangsung, serta kaitannya dengan aktifitas jaringan dalam kondisi operasional sehari-hari.

Kata Kunci — Network Behavior, Network Security, Anomaly Detection, Threat Classification