INTISARI

IMPLEMENTASI ALGORITME *K-MEANS CLUSTERING* DAN METODE *LEAST SQUARE* UNTUK PENILAIAN REPUTASI ALAMAT IP SECARA DINAMIS BERDASARKAN *BLACKLIST* ALAMAT IP

Saat ini, serangan pada jaringan internet sangat bermacam-macam dan jumlahnya meningkat setiap harinya. *Honeypot* terdistribusi atau MHN merupakan suatu sistem yang dapat digunakan untuk mengumpulkan informasi serangan, salah satu informasi yang didapat adalah informasi alamat IP penyerang. Agar dapat meyakinkan bahwa alamat IP tersebut merupakan alamat IP yang sangat berbahaya maka dibutuhkan suatu sistem penilaian. Pada penelitian ini akan dibuat suatu sistem yang dapat memberikan suatu informasi reputasi alamat IP secara dinamis dengan cara membandingkan alamat IP yang menyerang sensor MHN dengan 10 sumber *blacklist* alamat IP, kemudian alamat IP akan diamati kecenderungan atau tren dengan menggunakan metode *least square*. Tren tersebut akan digunakan untuk menentukan nilai reputasi dari alamat IP, setelah itu dengan algoritme *K-Means Clustering* alamat IP akan dikelompokkan dan diberi reputasi sesuai nilai yang diperoleh. Adanya sistem reputasi alamat IP yang dinamis ini, diharapkan alamat IP tidak selalu masuk ke dalam *blacklist* alamat IP sehingga yang tertampil hanya alamat IP yang dinilai sangat berbahaya, selain itu informasi reputasi alamat IP ini dapat dijadikan pertimbangan dalam membuat *policy* pada *firewall*.

Kata kunci: *Honeypot, Blacklist* IP*,* Metode *Least-Square*, algoritme *K-Means Clustering,* Reputasi alamat IP secara Dinamis

ABSTRACT

IMPLEMENTATION OF K-MEANS CLUSTERING ALGORITHM AND LEAST SQUARE METHOD FOR DETERMINING IP ADDRESS REPUTATION DYNAMICALLY BASED ON IP ADDRESS BLACKLIST

Currently, attacks to the Internet network is very diverse and the number increases every day. Distributed Honeypot or MHN is a system that can be used to collect about attacks information, one of the information that obtained is the attacker's IP address. To convince the attacker's IP address is dangerous, therefore needed IP address scoring system. In this research will be built system that give information about reputation of IP address dynamically. System will compare attacker IP address with 10 source blacklist IP and then the trend of attacker IP address will be observed with Least-square method to determine the score. The score will be grouped with K-Means Clustering algorithm and then given reputation. With this dynamic IP address reputation system, IP address is not always enter into blacklist IP, so that the information provided is only IP adddress that very dangerous and the information can be taken into consideration in creating a firewall policy.

Key word: Honeypot, Blacklist IP, K-Means Clustering algorithm, Least-square method, Dynamically IP Address Reputation