Implementasi MHN Server untuk mencegah serangan malware WannaCry dan DoS

Wahyu Nurohman[1], Niken Dwi Wahyu Cahyani[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]ubayebx@students.telkomuniversity.ac.id,
[2]nikencahyani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstrak

Jaringan komputer pada era sekarang memudahkan kita dalam pencarian informasi, tetapi tidak semua informasi terbuka untuk umum. *Malware* dalam bentuk *virus*, *rootkit*, dan *trojan horses* merupakan ancaman utama bagi keamanan sistem jaringan komputer. *Honeypot* merupakan salah satu metode dalam memperkuat keamanan jaringan yang bertujuan untuk mendeteksi kegiatan yang mencurigakan dan menjebak penyerang serta mencatat aktifitas yang dilakukannya. *Honeypot Dionaea* dan *Cowrie* membuat sistem layanan palsu layaknya sebuah server yang akan dijadikan pengalihan target utama serangan. Pada penelitian ini, implementasi jaringan dilakukan secara *virtual* sehingga dapat melakukan simulasi terhadap kinerja sistem dan merupakan suatu tantangan dalam memanfaatkan sumber daya perangkat yang terbatas. Pada penelitian ini akan dilakukan implementasi serangan *malware* kepada komputer server yang berbasis *Virtual Machine* menggunakan *VirtualBox*. Kemudian *malware* yang tersimpan oleh *Cowrie* dianalisis artifak datanya untuk melihat cara kerja *malware* tersebut, dengan diketahuinya artefak data dari *malware* yang tersimpan, maka tindakan yang tepat dapat segera dilakukan.

Kata kunci : Honeypot, Dionaea, Security, Rootkit, IDS

Abstract

Computer networks in this era are make easier for us to search for an information, but not all information is open to the public. Malware in the form of viruses, rootkits, and Trojan horses is a major threat to the security of computer network systems. Honeypot is a method of strengthening network security that aims to detect suspicious activities and trap the attacker and record the activities carried out. Dionaea and Cowrie Honeypot creates a fake service system like a server that will be used as a diversion for the main target of the attack. In this study, network implementation is done virtually so that it can simulate system performance and is a challenge in utilizing limited device resources. In this research, a rootkit malware attack will be implemented on Virtual Machine using VirtualBox. Then the malware stored by Cowrie will be analyzed its data artifacts to see how the malware works, knowing the data artifacts from the stored malware, the right action can be taken immediately.

Keywords: Honeypot, Dionaea, Security, rootkit, IDS.

1. Pendahuluan

Pada era teknologi sekarang yang semakin berkembang memudahkan kita dalam pencarian informasi, tetapi tidak semua informasi terbuka untuk umum. Oleh karena itu seiring perkembangan teknologi ini harus diiringi dengan sistem keamanan pada jaringan terhadap data atau informasi yang menggunakan internet supaya tidak terjadi pencurian data atau informasi penting. Pada tahun 2008 terdapat 3.534 celah pada sistem-sistem yang dengan mudahnya *attacker* melakukan penetrasi[6]. Pada tahun 2017 terjadi serangan *malware* dengan jenis *Ransomware* yang diberi nama *WannaCry* yang telah mengeskploit banyak komputer yang ada pada suatu perusahaan. *Intrusion Detection System*(IDS) adalah proses memonitor kegiatan yang berlangsung pada sebuah jaringan atau sistem komputer dan menganalisisnya untuk menandai bila terjadi suatu peristiwa yang mungkin terjadi, dimana pelanggaran atau ancaman yang mungkin terjadi dapat dideteksi dan diidentifikasi menggunakan kebijakan pada sistem keamanan komputer tersebut[4]. Tetapi apabila trafik pada suatu jaringan sangat tinggi sistem IDS akan sulit mengenali mana paket yang normal dan yang anomali karena kemampuan IDS hanya terbatas pada mengetahui adanya serangan yang masuk dalam bentuk *alert*, tanpa ada nya tindak lanjut. Dan untuk melengkapi sebuah