UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI HONEYPOT MENGGUNAKAN PLATFORM MODERN HONEY NETWORK (STUDI KASUS DI DIREKTORAT SISTEM
DAN SUMBER DAYA INFORMASI, UNIVERSITAS GADJAH MADA)**
WAHYU SEPTIAN , Warsun Najib, S.T., M.Sc. ; Ir. Sujoko Sumaryono , M.T.
Universitas Gadjah Mada, 2017 | Diunduh dari http://etd.repository.ugm.ac.id/

Intisari

Tindakan deteksi dan pencegahan dalam menangani resiko serangan pada infrastruktur jaringan dapat memanfaatkan alat bantu berupa *honeypot.* Metode kerja dan algoritma *honeypot* berbeda-beda tergantung jenisnya, dan telah melewati fase pengujian sebagai alat mitigasi serangan. *Honeypot* yang bekerja sendiri tanpa adanya integrasi satu dengan yang lain dapat menimbulkan dampak negatif yang lain, diantaranya adalah kesulitan dalam mengelola *event* yang tertangkap *honeypot* tersebut. Penelitian ini bertujuan meng-integrasikan berbagai sensor *honeypot* yang terpasang di lingkungan DSSDI UGM ke dalam sebuah *platform* pengelola *event* yang berjalan pada satu server terpadu.

Metode penelitian yang dilakukan pada penelitian ini adalah dengan melakukan instalasi *platform* MHN ke dalam satu perangkat server fisik. Pengembangan sensor *Kippo* SSH, Dionaea, p0f dan *snort* dilakukan melalui *dashboard* utama yang terdapat pada *platform* MHN dengan menggunakan *script* yang dibuat oleh server tersebut. *Script* yang didapatkan selanjutnya disalin untuk dijalankan pada *command* terminal pada perangkat sensor dengan sistem operasi berbasis debian. Server utama MHN diintegrasikan lagi dengan *platform* ELK sebagai alat dalam mengelola data *malicious activity* yang telah tertangkap oleh sensor yang telah diintegrasikan sebelumnya.

Dari penelitian yang dilakukan, didapat hasil data *malicious activity* yang telah diolah oleh antarmuka Kibana diantaranya adalah: asal serangan, tujuan serangan, Negara penyerang, *port* tujuan serangan, *username* beserta *password* yang digunakan selama serangan berlangsung. Alamat IP penyerang yang paling banyak melakukan penyerangan selama penelitian berlangsung adalah **163.172.202.221** dengan serangan sebanyak **12,795** kali. Penelitian ini merekomendasikan untuk melakukan pemblokiran akses terhadap alamat ip yang banyak melakukan serangan. Tujuan penyerangan paling banyak selama penelitian berlangsung adalah perangkat dengan alamat IP **202.43.92.54** (DSSDI UGM) dengan serangan sebanyak **69,622** kali. Sensor telah mencatat bahwa serangan yang berasal dari Negara ***Croatia*** telah melakukan **19,717** kali serangan menempati peringkat pertama. Peringkat pertama *port* tujuan serangan selama penelitian dilakukan adalah *port* **5060** (layanan SIP) tercatat **43,418** kali, dan untuk *port* **22** (layanan ssh) tercatat **14,346** kali serangan atau pada peringkat ke-tiga. *Username* yang digunakan dalam proses serangan adalah "*root*" terhitung sebanyak **6,601** kali penggunaan, sedangkan *password* yang digunakan dalam proses serangan adalah "*admin"* tercatat sebanyak **245** kali penggunaan. Penelitian ini merekomendasikan untuk menghindari penggunaan *username* dan *password* yang menjadi tren selama penelitian berlangsung.

Kata kunci : Manajemen Even, *Honeypot*, *Modern Honey Network*, ELK.

UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI HONEYPOT MENGGUNAKAN PLATFORM MODERN HONEY NETWORK (STUDI KASUS DI DIREKTORAT SISTEM
DAN SUMBER DAYA INFORMASI, UNIVERSITAS GADJAH MADA)**
WAHYU SEPTIAN , Warsun Najib, S.T., M.Sc. ; Ir. Sujoko Sumaryono , M.T.
Universitas Gadjah Mada, 2017 | Diunduh dari http://etd.repository.ugm.ac.id/

Abstract

Detection and prevention actions in dealing with the risk of attacks on the network infrastructure can leverage tools such as honeypot. The working methods of honeypot and its algorithms may vary according to its kind, and honeypot has passed the testing phase for which mitigating the attack. The stand-alone honeypot who work individually without integration to each other may have negative impacts in advance, which is difficulty in managing the event captured by the honeypot itself. This study aims to integrating various network sensors and honeypot that installed in the environment of DSSDI UGM into an event management platform that runs on integrated server.

The research method in this study is to perform the installation of MHN platform into a single physical server device. Sensor development such as Kippo SSH, Dionaea, p0f and snort carried out through the main dashboard which is contained in MHN platform by using a script created by the server. Script that obtained from main server copied to a command terminal at a sensor device with a debian operating system based. MHN main servers are integrated with the platform again ELK as a tool in managing data of malicious activity that has been captured by the sensor that has been integrated before.

From the research conducted, the result data of malicious activity that has been processed by the interface of Kibana, among them are: the origin of the attacks, the destination of the attack, the State of attacker, attack destination port, username and password that is used during the attack. IP address of the attacker who had done many attacks during the study was ***163.172.202.221*** *(1st rank of the attacker) and the attack amount was* ***12.795*** *times. This study recommends to blocking access to ip addresses that did many attacks. Destination of attack at most during the study is the device with the IP address* ***202.43.92.54*** *(DSSDI UGM) and attacked as much as* ***69.622*** *times. Sensors have noted that attacks originating from Country Croatia has made* ***19.717*** *times and ranked at first attack. The first rank destination port attacks during the study done is port* ***5060*** *(SIP service) recorded* ***43.418*** *times, and to port* ***22*** *(ssh service) recorded* ***14.346*** *attacks or at 3rd rank. Username used in the attack was the "root" counted as many as* ***6.601*** *times of use, while password used in the attack was "admin" recorded as many as* ***245*** *times of use. This study recommends avoiding the usage of usernames and passwords to be the trend during the study.*

Keywords : *Event Management, Honeypot, Modern Honey Network, ELK.*