INTISARI

IMPLEMENTASI HONEYPOT SEBAGAI PEMANTAUAN PARAMETER PADA HTTP REQUEST UNTUK MENGETAHUI TUJUAN SERANGAN

Layanan dan aplikasi internet semakin banyak dimanfaatkan. Komunikasi aplikasi internet menggunakan protokol HTTP yang disepakati berjalan pada port 80 dan 443. Berbagai serangan terhadap *web server* dapat dijalankan melalui port 80. Beberapa serangan tersebut antara lain: *injection*, kesalahan manajemen *session*, XSS, kesalahan pengaturan keamanan, *cross-side request forger* dan, pengalihan halaman. Ancaman-ancaman tersebut ada yang berasal dari sisi *client* maupun dari *server*. Salah satu model ancaman yang berasal dari *client* dapat terjadi pada manipulasi parameter yang dikirim melalui HTTP *request*.

Honeypot merupakan sistem yang sengaja dibangun untuk diselidiki, diserang ataupun dikompromikan. Salah satu jenis *honeypot* adalah Glastopf. *Honeypot* Glastopf merekam akses yang masuk pada *web server* umpan. Kemudian data yang tersimpan dianalisis jenis serangannya. *Honeypot* dengan tingkat interaksi rendah seperti glastopf dapat dikelola dan diintegrasikan dengan honeypot lain menggunakan MHN. Pada tugas akhir ini meneliti bentuk serangan yang dilakukan dari HTTP *request. Honeypot* Glastopf diterapkan pada *server* jaringan internet di Kampus UGM untuk merekam data. MHN dibantu HIHAT mengelola dan memvisualkan data serangan yang terjadi. Hasilnya terlihat parameter-parameter serangan yang dikirimkan penyerang dan diketahui tujuan serangannya.

Kata Kunci : *Honeypot*, Glastopf, Modern Honey Network, HTTP *request*

ABSTRACT

IMPLEMENTATION OF A HONEYPOT TO MONITOR PARAMETERS OF HTTP REQUEST FOR ATTACK ANALYSIS

Services and internet application are increasingly being used. Internet application communications using HTTP protocol that agreed run on ports 80 and 443. Various attacks on the web server can be run on port 80. Some of these attacks, i.e: injection, session management error, XSS, security setting errors, cross-side request forger and page redirection. The threats are coming from the client or server side. Client can manipulate the parameters that sent over HTTP requests.

Honeypot is a system that is intentionally built to investigated, attacked or compromised. One type of honeypot is Glastopf. Glastopf Honeypot records incoming access on the bait server web. Then the data stored analyzed the type of attack. Honeypots with low interaction levels such as glastopf can be managed and integrated with other honeypot using MHN. In this thesis examine kind of attacks carried out from HTTP request. Glastopf Honeypot applied on the internet network server at UGM campus to record the data. MHN assisted HIHAT manage and visualize attack data that happened. The results show the attack parameters sent by the attacker and known the purpose of the attack.

Keyword : Honeypot, Glastopf, Modern Honey Network, HTTP request