ANALYSIS AND IMPLEMENTATION OF HONEYPOT USING KIPPO AS A SUPPORTING NETWORK SECURITY

[1]Tri Handoyo Saputro, [2]Triawan Adi Cahyanto, [3]Hardian Oktavianto
Department of Informatics Faculty of Engineering
University Muhammadiyah Jember
akun.lawas@gmail.com

ABSTRACT

Honeypot is a system that is built to resemble the actual system, with the aim that the attacker distracted from the main system to be in attack, and switch the attack to a false system. Kippo Honeypot is one that includes the category of low-Interaction Honeypot. Kippo it self is a program designed using python programming language to emulate shell. In this research with the analysis and implementation Kippo honeypot that can provide activity reports brute-force attack to administrators, so it can detect attacks against the network.

Brute-force technique is an old technique that is often a mainstay of the perpetrators of cybercrime in finding the right main access to a computer application. Brute-force works by menginputkan all combinations of usernames and passwords randomly in large quantities and within a short time to get a username and password combinations that are already recorded by the system to be attacked.

Keywords *: Honeypot, Kippo, Brute-force ,Virtual host*

ANALISIS DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN KIPPO SEBAGAI PENUNJANG KEAMANAN JARINGAN

[1]Tri Handoyo Saputro, [2]Triawan Adi Cahyanto, [3]Hardian Oktavianto
Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember
akun.lawas@gmail.com

ABSTRAK

Honeypot merupakan sebuah sistem yang di bangun menyerupai dengan sistem yang sesungguhnya dengan tujuan agar para *attacker* teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut. *Kippo Honeypot* merupakan salah satu yang termasuk kategori *low-Interaction Honeypot. Kippo* sendiri merupakan sebuah program yang dirancang menggunakan bahasa pemrograman python untuk mengemulasi shell. Pada penelitian ini berkaitan dengan analisis dan implematasi *honeypot kippo* yang mampu memberikan laporan aktivitas serangan brute-force kepada administrator,sehingga dapat mendeteksi serangan yang terjadi terhadap jaringan.

Teknik *brute-force* memang merupakan sebuah teknik usang yang masih sering menjadi andalan para pelaku *cybercrime* dalam mencari hak akses utama menuju suatu aplikasi komputer. *Brute force* bekerja dengan cara menginputkan semua kombinasi *username* dan *password* secara acak dalam jumlah banyak dan dalam kurun waktu yang cepat untuk mendapatkan kombinasi *username* dan *password* yang memang telah tercatat oleh sistem yang akan diserang.

Kata Kunci *: Honeypot, Kippo, Bruteforce ,Virtual host*

I. PENDAHULUAN

1.1 Latar Belakang

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan Internet dalam segala bidang *seperti e-banking, e-commerce, e-government*, *e-education* dan lain sebagainya telah menjadi sesuatu yang tidak asing lagi. Untuk itu pemanfaatan jaringan internet untuk memudahkan komunikasi antar manusia di dunia sudah sangat meluas. Misalnya saja penggunakan internet pada media sosial, media pemberitaan, media jual-beli, dan media lainnyayang dilakukan secara *online.* Di mana kita ketahui media – media tersebut merupakan media penghubung antar banyak pihak dan juga merupakan media yang memungkinkan untuk dapat diakses oleh semua orang melalui internet. Dengan semakin tingginya tingkat kompleksitas penggunaan jaringan komputer, maka semakin tinggi pula ancaman yang ada. Misalnya saja untuk mengambil alih hak akses komputer lain sebagai *user*, penyerang dapat melakukan kontrol jarak jauh atau *remote* melalui *port* ssh dari komputer yang akan di-*remote*.

Untuk itu dalam penelitian ini akan dikembangkan sebuah *kippo honeypot* yang merupakan emulasi dari *port* ssh. Teknik *brute-force* memang merupakan sebuah teknik usang yang masih sering menjadi andalan para pelaku *cybercrime* dalam mencari hak akses utama menuju suatu aplikasi komputer. *Brute force* bekerja dengan cara menginputkan semua kombinasi *username* dan *password* secara acak dalam jumlah banyak dan dalam kurun waktu yang cepat untuk mendapatkan kombinasi *username* dan *password* yang memang telah tercatat oleh sistem yang akan diserang.

Pada tugas akhir ini berkaitan dengan analisis dan implematasi *honeypot kippo* yang mampu memberikan laporan aktivitas serangan jaringan kepada administrator, sehingga dapat dipelajari pola serangan yang terjadi terhadap jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada maka dapat dirumuskan berapa pemasalahan yang ada yaitu :

1. Bagaimana mengimplementasikan *Honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan?
2. Bagaimana melakukan analisa kinerja *honeypot* menggunakan *kippo* terhadap serangan *attacker*?

1.3 Tujuan Penelitian

Adapun tujuan dari tugas akhir ini antara lain:

1. Merancang dan menciptakan *honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan.
2. Melakukan analisa kinerja *honeypot* menggunakan *kippo* terhadap serangan *attacker*.

II. TINJAUAN PUSTAKA

2.1 Honeypot

Honeypot merupakan sebuah sistem yang di bangun menyerupai atau persis dengan sistem yang sesungguhnya, dengan tujuan agar para *attacker* teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut. Saat ini *honeypot* tidak hanya berfungsi atau bertujuan untuk bertujuan menjebak *attacker* untuk melakukan serangan ke *server* asli, namun *honeypot* juga bermanfaat untuk para *system administrator* atau *security analyst*, untuk menganalisa aktifitas apa saja yang dilakukan oleh *atacker* / *malware* yang terdapat di dalam sistem *honeypot* tersebut.

Honeypot dapat diklasifikasikan berdasarkan pada tingkat interaksi yang dimilikinya. Tingkat interaksi dapat didefinisikan sebagai tingkat aktivitas penyerang didalam sistem yang diperbolehkan maka semakin tinggi pula tingkat interaksi *honeypot*.

1. Low Interaction Honeypot

Low-interaction honeypot merupakan honeypot yang didesain untuk mengemulasikan *service* (layanan) seperti pada *server* yang asli. Misalnya hanya *service* FTP, Telnet, HTTP, dan *service* lainnya.

2. High Interaction Honeypot

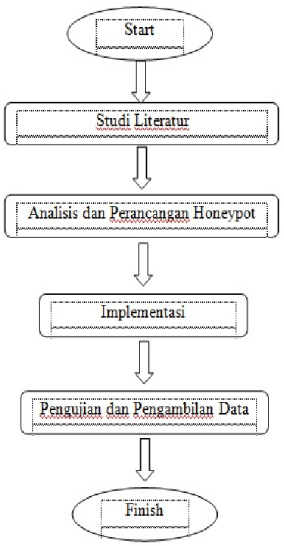
High-interaction honeypot merupakan tipe *honeypot* dimana menggunakan keseluruhan *resource* sistem, dimana *honeypot* ini benar-benar persis seperti sistem yang asli. *Honeypot* jenis ini bisa berupa satu keseluruhan *operating system*.

2.2 Kippo

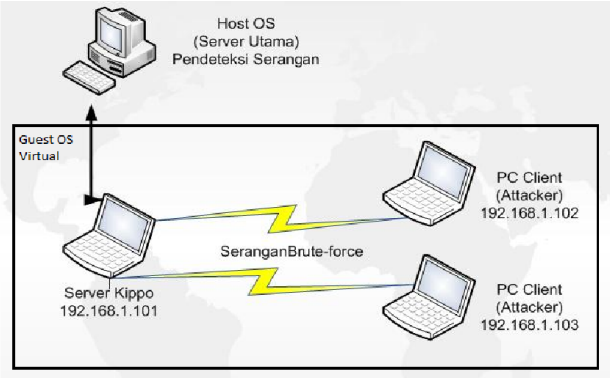
Kippo honeypot salah satu *honeypot* yang termasuk kategori *Low-Interaction Honeypot. Kippo Honeypot* adalah sebuah program yang dirancang menggunakan bahasa pemrograman *python* untuk mengemulasi *shell*. *Kippo honeypot* bekerja tidak hanya sebegai pendeteksi serangan *brute-force*, tetapi juga bekerja layaknya *ssh server* yang asli dengan menyediakan beberapa layanan interaksi bagi penyerang berupa perintah-perintah *ping, ssh, wget* dan lain-lain.

III. METODE PENELITIAN

3.1 Konsep Penelitian



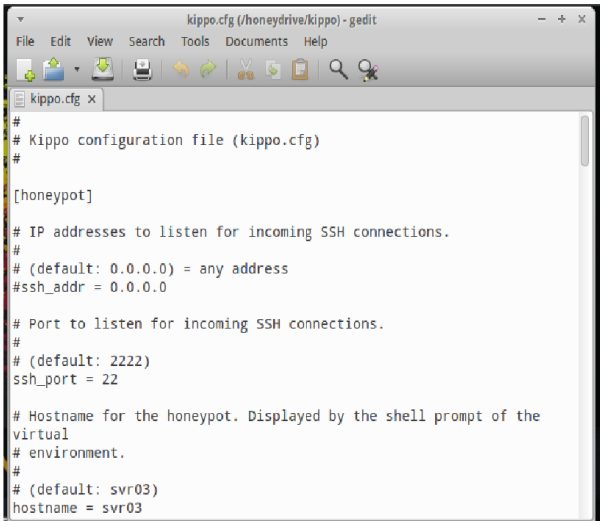
3.2 Topologi Jaringan



IV. HASIL DAN PEMBAHASAN

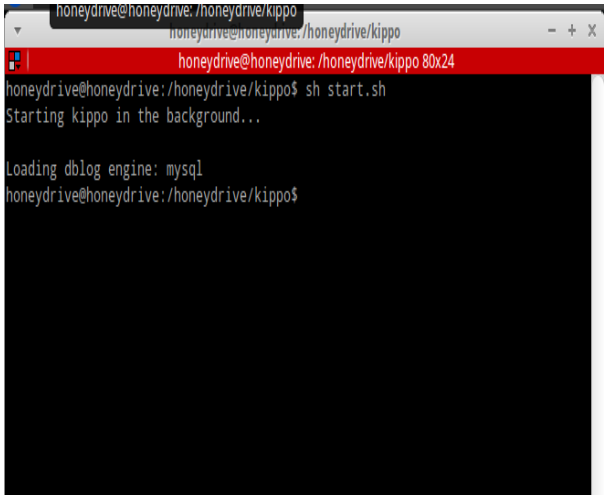
4.1 Konfigurasi Kippo

Konfigurasi ini menjelaskan bahwa sistem secara default, Kippo menggunakan port 2222 sebagai port standar, karena kita ingin menggunakan port 22 sebagai port Kippo kita dapat mengganti port standar tersebut pada file konfigurasi. Langkah pertama kita edit file kippo.cfg dengan mengetikkan perintah gedit kippo.cfg lalu akan muncul teks editor yang akan kita ubah seperti gambar dibawah ini



4.2 Menjalankan kippo

Pada tahap ini kippo yang sebelumnya telah dikonfigurasi akan dijalankan dan siap diserang oleh attacker.



4.3 Pengujian Serangan

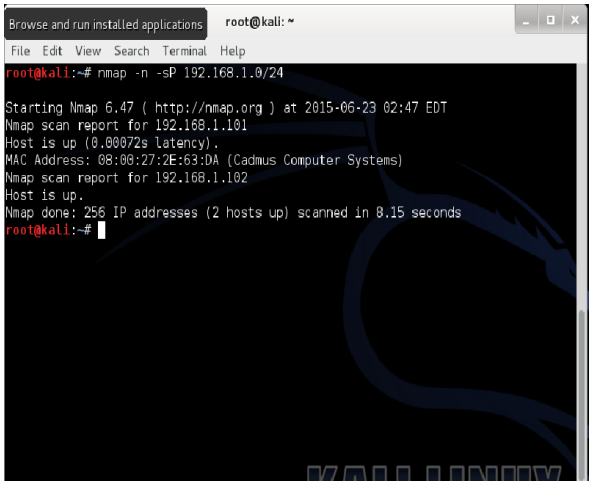
Pengujian Scanning Host dan Port

Dalam suatu proses awal pada kegiatan *hacking*, yang bertujuan menemukan dan mengumpulkan sebanyak mungkin informasi tentang target. Adapun skenario pengujian keberhasilannya adalah sebagai berikut :

1. Melakukan *scanning host* aktif dan lakukan ping terhadap host aktif untuk menunjukkan bahwa host benar-benar dalam keadaan aktif.
2. Melakukan *scanning port*

Scanning Host

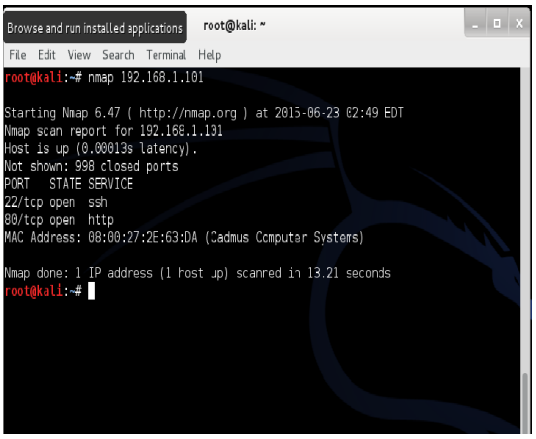
Pengujian pertama yaitu melakukan scanning host. Proses scanning berfungsi untuk mengetahui informasi mengenai host yang aktif yang salah satunya adalah honeypot. Dengan cara melakukan perintah nmap –n –sP 192.168.1.0/24 pada *terminal* seperti terlihat pada gambar dibawah



Terlihat pada gambar diatas Proses *scanning host* menggunakan nmap diketahui ada 2 host yang aktif.

Scanning Port

Pengujian yang kedua yaitu scanning port, melakukan proses scanning port yang bertujuan untuk mengetahui port mana saja yang telah terbuka. Menggunakan aplikasi nmap untuk mengetahui port-port mana saja yang terbuka pada masing-masing honeypot, Proses ini terlihat pada gambar

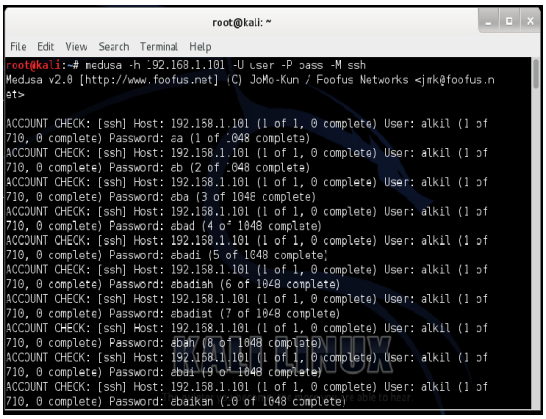


Pengujian Serangan Bruteforce

Pengujian bruteforce dilakukan menggunakan aplikasi medusa. Dalam pengujian ini attacker melakukan bruteforce dengan tujuan untuk melakukan remote komputer server dari komputer client.

Bruteforce pada port SSH

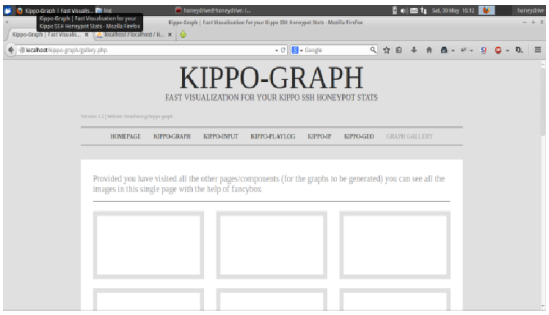
Serangan *bruteforce* pada port SSH ini dilakukan dengan teknis memberikan serangan pada salah satu honeypot dengan cara mengetikkan perintah pada terminal yaitu : medusa –h <host> -U <user> –P <password> -M ssh



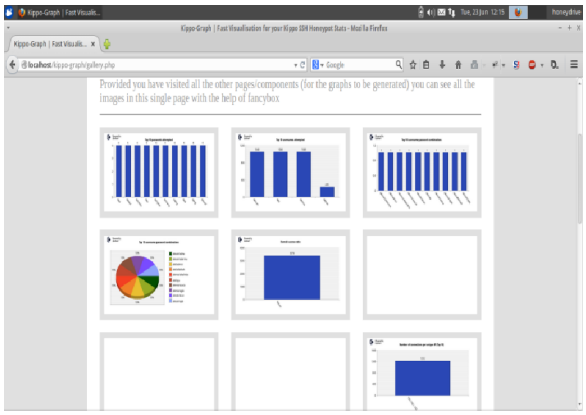
Dari hasil pada gambar diatas serangan *bruteforce* tidak berhasil mendapatkan *password* pada serangan *port* SSH dengan alamat IP 192.168.1.101

4.4 Analisa Aktivitas Serangan Dengan Kippo-Graph

Berikut merupakan hasil dari aktivitas serangan terhadap *honeypot* dengan menggunakan *web interface* yaitu Kippo-Graph. Dengan mengakses melalui *browser* yaitu : localhost/kippo-graph terlihat pada gambar dibawah adalah tampilan awal *web interface* kippo-graph berupa grafik, diagram dan lain sebagainya.



Pada gambar diatas terlihat tampilan awal *log web interfaces* menggunakan kippo-graph sebelum terjadi serangan, dapat dilihat belum ada peningkatan pada grafik dan diagram semuanya masih kosong sesuai default dan pada gambar dibawah dapat diamati perubahan telah terjadi dapat dilihat pada grafik dan diagramnya inilah kondisi setelah dilakukan serangan.



V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan implementasi dan pengujian yang telah dilakukan pada bab sebelumnya maka dapat disimpulkan sebagai berikut :

1. Berdasarkan skenario uji coba sistem, implementasi *Kippo* dapat membaca setiap serangan dari *attacker* dan mampu mendeteksi serangan *brute-force* sesuai indikator serangan yang dicantumkan pada penelitian ini.
2. Dalam penggunaan *honeypot* ini dapat melindungi *resource* utama dari percobaan serangan yang dilakukan oleh pihak ekstenal (*attacker*).

5.2 Saran

Untuk pengembangan selanjutnya, diharapkan sistem dapat mengenali parameter terjadinya serangan *brute – force* dalam jumlah banyak dan bervariasi dan juga sistem bisa mengklasisfikasikan jenis serangan *brute – force* ataupun *non-brute-force.*

DAFTAR PUSTAKA

Hadistira, Hafid (2015) "Analisa dan Implementasi Honeypot Menggunakan Honeyd Sebagai Penunjang Keamanan Jaringan" Universitas Muhammadiyah Jember.

Muh Masruri Mustofa, (2013) "*Penerapan Sistem Keamanan Honeypot Dan Ids Pada Jaringan Nirkabel (Hotspot)*", Program Studi Teknik Informatika Universitas Ahmad Dahlan, Yogyakarta

Nurhasanah Umayah, "*Perancangan dan Implementasi Honeypot* pada *Virtual Private Server sebagai Penunjang Keamanan Jaringan*" Politeknik Telkom.

Sugeng, W. (2010). Jaringan Komputer dengan TCP/IP. Bandung: Modula

Syafrizal, Melwin (2005) “Pengantar Jaringan Komputer” . Yogyakarta: Penerbit Andi

Utdirartatmo, F. (2005). Menjebak Hacker dengan Honeypot. Yogyakarta:

Andi.

Copyright @2015 Unixmen, diakses tanggal 06 mei 2015. http://www.unixmen.com/kippo-ssh-honeypot-monitor-brute-force-attacks-debian-7-ubuntu-13-10/

Foofus, “Medusa Parallel Network Login Auditor” Diakses tanggal 07 Mei 2015. http://foofus.net/goons/jmk/medusa/medusa.html

Virtual Private Server, Diakses Januari 22, 2015 dari http://www.indonic.net/

vps-hosting/

Wikipedia, “Nmap(Nmap Security Scanner)” Diakses tanggal 07 Mei 2015. http://en.m.wikipedia.org/wiki/Nmap