ANALISA DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN HONEYD SEBAGAI PENUNJANG KEAMANAN JARINGAN

Hafid Hadistira (1010651087)
Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember
hafid.hadistira@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. *Honeyd* adalah sebuah produk *honeypot* yang ditulis oleh Niels Provos. Inti dari *Honeyd* adalah sistem ini akan mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya. Honeyd memiliki kemampuan untuk mensimulasikan TCP dan UDP selain itu sistem ini mampu memahami dan merespon ICMP dengan baik,serta memiliki kemampuan untuk membuat *virtual honeypot* dengan alamat IP yang banyak secara bersamaan.

Pada tugas akhir ini akan dibangun sebuah sistem *Honeypot* menggunakan *Honeyd*. Kemudian sistem yang dibangun akan dilakukan pengujian simulasi penyerangan menggunakan teknik *Footprinting*, DoS dan *Bruteforce*. Dari hasil pengujian terbukti bahwa tidak terjadi serangan pada *server* asli dengan IP Address 192.168.1.1 tetapi serangan terjadi pada 3 *virtual host* yang diciptakan oleh *honeyd* yaitu IP Address 192.168.1.2 sebanyak 28%, 192.168.1.3 sebanyak 51% dan 192.168.1.4 sebanyak 21%.

***Kata Kunci** : Honeypot, Honeyd, Footprinting, DoS, Bruteforce ,Virtual host*

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

Hafid Hadistira (1010651087)
Department of Informatics Faculty of Engineering, Univesity Muhammadiyah Jember
hafid.hadistira@gmail.com

ABSTRACT

Honeypot is a system that is built to resemble the actual system with the goal of keeping the attacker distracted from the main system to be attacked, and switch the attack to the fake system. Honeyd is a honeypot product written by Niels Provos. The point of Honeyd is this system will simulate the behavior of a computer and its operating system. Honeyd has the ability to simulate TCP and UDP in addition the system is able to understand and respond to ICMP well, and has the ability to create a virtual honeypot with the IP address that many simultaneously.

In this final project will be built a Honeypot system using Honeyd. Then the system will be be tested using techniques Footprinting, DoS and bruteforce. From the test results proved that there was no attack on the real server with IP address 192.168.1.1 but the attack occurred at 3 virtual hosts created by Honeyd is the IP address 192.168.1.2 as much as 28%, 192.168.1.3 as much as 51% and 192.168.1.4 as much as 21 %.

***Keywords** : Honeypot, Honeyd, Footprinting, DoS, Bruteforce ,Virtual host*

I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunanannya, membawa banyak dampak baik yang bersifat positif maupun yang bersifat negatif. Dampak positif misalnya jaringan Internet saat ini dapat membantu manusia untuk saling berkomunikasi serta bertukar informasi, Namun tidak sedikit juga dampak negatif yang ditimbulkan karena adanya Internet, misalnya seorang *hacker* dapat masuk ke dalam suatu sistem jaringan untuk mencuri data dan informasi penting. Maka dari itu diperlukan adanya sistem keamanan jaringan komputer.Salah satu metode untuk mengamankan jaringan adalah dengan *Honeypot*.

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. *Honeyd* adalah sebuah produk *honeypot* yang ditulis oleh Niels Provos. Inti dari *Honeyd* adalah sistem ini akan mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya. Honeyd memiliki kemampuan untuk mensimulasikan TCP dan UDP selain itu sistem ini mampu memahami dan merespon ICMP dengan baik,serta memiliki kemampuan untuk membuat *virtual honeypot* dengan nomor IP yang banyak secara bersamaan.

Pada penelitian ini akan dibangun sebuah sistem *Honeypot* menggunakan *Honeyd* 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 :

Bagaimana mengimplementasikan metode *Honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan?

Bagaimana melakukan analisa kinerja *honeypot* menggunakan *honeyd* terhadap serangan yang dilakukan oleh *attacker*?

1.3 Batasan Masalah

Untuk pembuatan tugas akhir ini agar sesuai dengan judul yang telah dibuat, maka penulis akan memberikan batasan-batasan masalah yang akan dibahas yaitu: Honeypot ini akan dibangun menggunakan aplikasi honeyd yang akan mengemulasikan 3 virtual host.Setelah sistem selesai dibangun maka akan dilakukan pengujian dengan serangan Footprinting, DoS dan Bruteforce

1.4 Tujuan Penelitian

Mengimplementasikan *Honeypot* Menggunakan *Honeyd* Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan.

Melakukan analisa kinerja *honeypot* menggunakan *honeyd* terhadap serangan yang dilakukan oleh *attacker*.

1.5 Manfaat Penelitian

Dapat memberikan gambaran tentang kinerja metode *Honeypot* sebagai sistem keamanan jaringan komputer.

Dapat memberikan informasi kepada administrator jaringan tentang teknik atau pola-pola serangan yang digunakan oleh *attacker* yang nantinya akan dianalisa lebih lanjut untuk menemukan solusi yang tepat dalam menangani keamanan suatu jaringan komputer.

Manfaat lainnya dapat di jadikan acuan untuk pengembangan selanjutnya dengan menggunakan teknologi yang berbeda-beda.

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

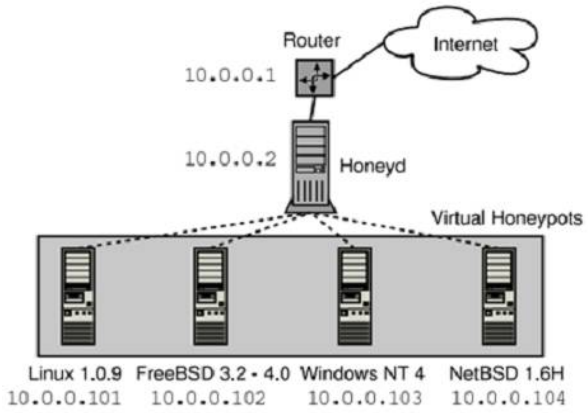
Low-interaction honeypot merupakan honeypot yang didesain untuk mengemulasikan *service* (layanan) seperti pada *server* yang asli. Misalnya hanya *service* FTP, Telnet, HTTP, dan *service* lainnya.

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*.

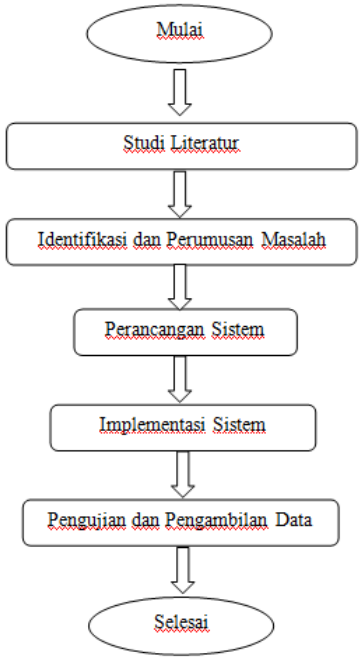
2.2 Honeyd

Honeyd adalah sebuah produk *honeypot* dengan *tipe low interaction*. Inti dari *Honeyd* adalah sistem ini akan mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya. Pada saat yang sama kita dapat mengkonfigurasi sistem-sistem operasi untuk mengaktifkan layanan seperti FTP, HTTP, Telnet, dan lain-lain. *Honeyd* memiliki kemampuan untuk mensimulasikan TCP dan UDP, mampu memahami dan merespon ICMP dengan baik, dan memiliki kemampuan untuk membuat *virtual honeypot* dengan nomer IP yang banyak secara bersamaan.

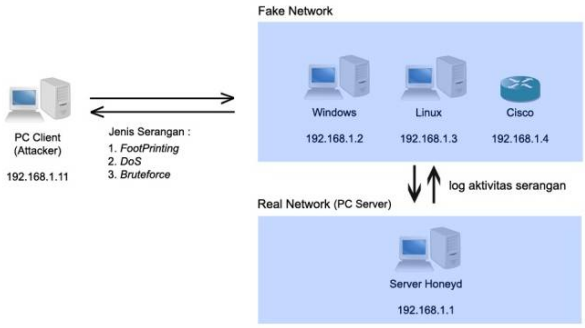


III. METODE PENELITIAN

3.1 Konsep Penelitian



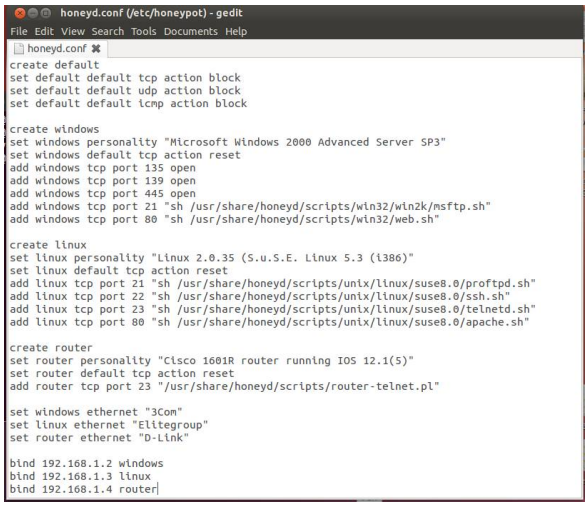
3.2 Topologi Jaringan



IV. HASIL DAN PEMBAHASAN

4.1 Konfigurasi Honeyd

Konfigurasi *honeyd* ini dilakukan dengan tujuan untuk membuat sistem operasi beserta layanan yang diberikan kepada penyerang. *Honeypot* disini dibuat dengan tujuan memberikan sumber daya atau informasi palsu kepada penyerang sehingga *administrator* dapat menganalisa maksud dan tujuan dari penyerang.



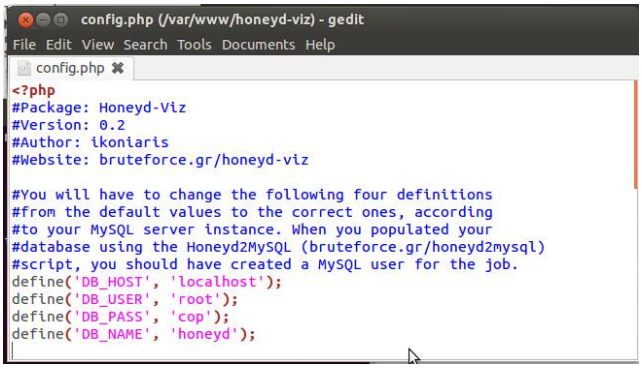
Dapat dilihat pada gambar diatas merupakan file konfigurasi honeyd untuk membuat 3 *virtual host* yaitu Windows,Linux dan Router Cisco. Berikut keterangannya :

1. create : untuk inisialisasi pembuatan *virtual honeypot*.
2. set : untuk pemberian personality pada *virtual honeypot*.
3. add : untuk mendefinisikan perlakuan default protokol jaringan.
4. bind : melakukan pemberian alamat IP untuk setiap *virtual honeypot*.

4.2 Konfigurasi Honeyd-viz

Konfigurasi *honeyd-viz* ini dilakukan untuk mempermudah *administrator* dalam menganalisa hasil serangan pada *honeyd*. Adapun langkah-langkah konfigurasi *honeyd-viz* adalah :

1. wget http://bruteforce.gr/wp-content/uploads/honeyd-viz-0.2.
2. mv honeyd-viz-0.2.tar /var/www
3. cd /var/www
4. tar xvf honeyd-viz-0.2.tar - -no-same-permissions
5. cd honeyd-viz
6. chmod 777 generated-graphs
7. gedit config.php



Terlihat pada gambar 4.5 merupakan file konfigurasi *honeyd-viz*, rubah *script* akun *database* yang terdiri dari DB_HOST, DB_USER, DB_PASS, DB_NAME dengan konfigurasi *database* pada MySql.

4.3 Pengujian Serangan

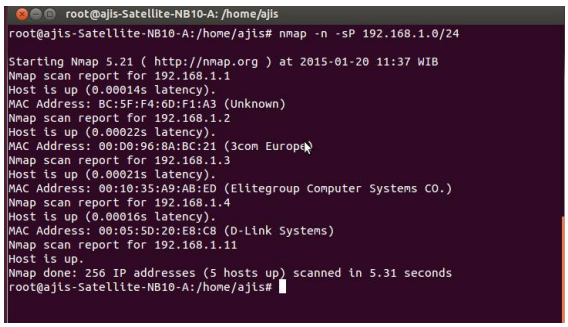
Pengujian Serangan Footprinting

Footprinting adalah suatu proses awal pada kegiatan *hacking*, yang bertujuan menemukan dan mengumpulkan sebanyak mungkin informasi tentang target. Adapun skenario pengujian keberhasilan dari *footprinting* 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

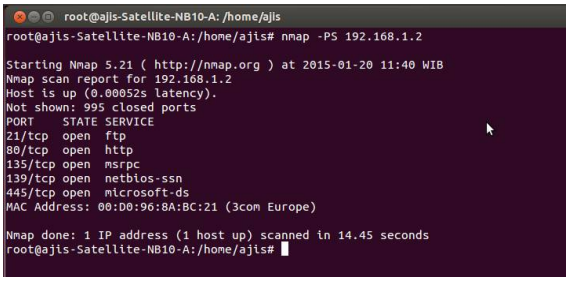
Pengujian pertama yaitu melakukan *scanning host*. Proses *scanning* berfungsi untuk mengetahui informasi mengenai host yang aktif yang salah satunya adalah *honeypot*. Dengan cara melakukan perintah nmap –n –sP 192.168.1.0/24 pada *terminal* seperti terlihat pada gambar dibawah

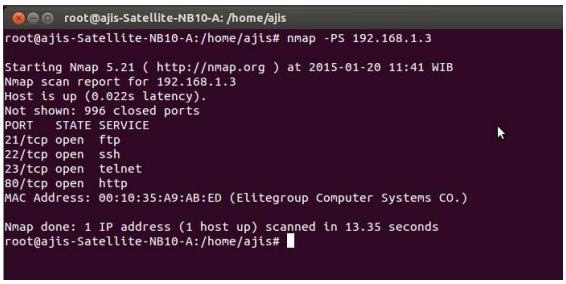


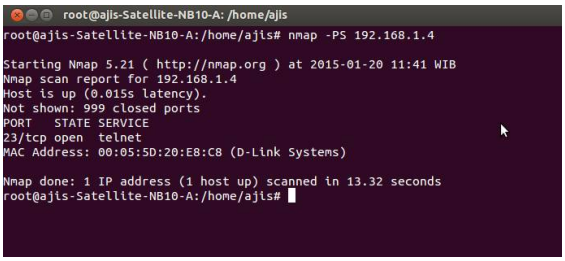
Terlihat pada gambar diatas Proses *scanning host* menggunakan nmap diketahui ada 5 host yang aktif beserta mac address nya.

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*.







Pengujian Sernngan DoS

DoS merupakan serangan yang dilancarkan melalui paket-paket tertentu. Bentuk serangan yang akan digunakan dalam pengujian antara lain ping attack dan syn attack.

Ping Attack

Serangan *ping attack* ini dilakukan dengan cara mengirim paket ICMP yang berlebih secara berturut-turut terhadap *server*. Tujuan penyerangan ini membuat sistem menjadi *crash* dan *hang*. untuk melakukan serangan ini, penyerang menggunakan *terminal* dengan cara ping -f -s <size> <host>.

Pada gambar diatas terlihat *attacker* melakukan serangan *ping attack* kepada *honeypot* yaitu ke alamat 192.168.1.2 dimana jumlah paket yang dikirim berjumlah 1500 byte.

Syn Attack

Serangan yang dilakukan dengan menyerang lubang keamanan dari implementasi *protocol* TCP/IP dengan menggunakan aplikasi hping3. Sama dengan serangan *ping attack* tujuan serangan *syn attack* ini membuat sistem menjadi *crash* dan *hang*. Teknis penyerangan ini adalah dengan mengetikkan pada *terminal* hping3 -i ul -S<host>-p <port>-d<size>

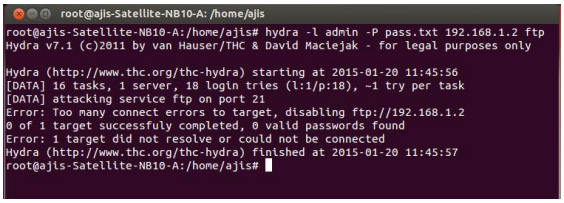
Pada gambar diatas terlihat *attacker* melakukan serangan *syn attack* dengan aplikasi hping3 kepada *honeypot* yaitu ke alamat 192.168.1.4 dimana jumlah paket yang dikirim berjumlah 60000 byte.

Pengujian Serangan Bruteforce

Pengujian *bruteforce* dilakukan menggunakan aplikasi hydra. Dalam pengujian ini *attacker* melakukan *bruteforce* pada port *FTP*, *telnet*, dan *SSH* dengan tujuan untuk melakukan remote komputer server dari komputer client.

Bruteforce pada port FTP

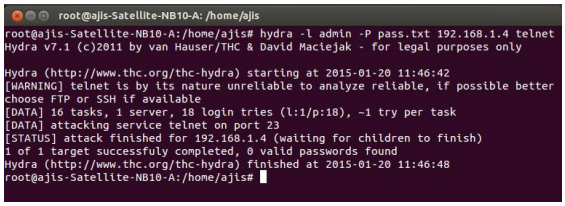
Serangan *bruteforce* pada port FTP ini dilakukan dengan teknis memberikan serangan pada salah satu *honeypot* dengan cara mengetikkan perintah pada *terminal* yaitu : hydra -l <user> -P <directory password> <host> ftp.



Dari hasil pada gambar diatas serangan *bruteforce* tidak berhasil mendapatkan *password* pada serangan port FTP dengan alamat IP 192.168.1.2.

Bruteforce pada port Telnet

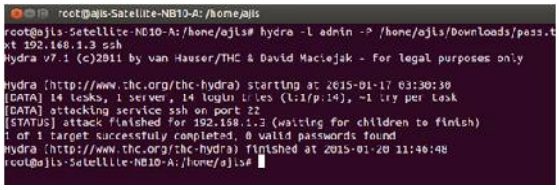
Serangan *bruteforce* pada port telnet ini dilakukan dengan teknis memberikan serangan pada salah satu *honeypot* dengan cara mengetikkan perintah pada *terminal* yaitu : hydra –l <user> –P <directory password> <host> telnet.



Dari hasil pada gambar diatas serangan *bruteforce* tidak berhasil mendapatkan *password* pada serangan port telnet dengan alamat IP 192.168.1.4.

Bruteforce pada port SSH

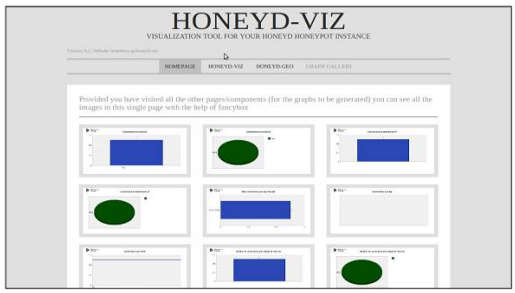
Serangan *bruteforce* pada port SSH ini dilakukan dengan teknis memberikan serangan pada salah satu *honeypot* dengan cara mengetikkan perintah pada *terminal* yaitu : hydra –l <user> –P <directory password> <host> ssh.



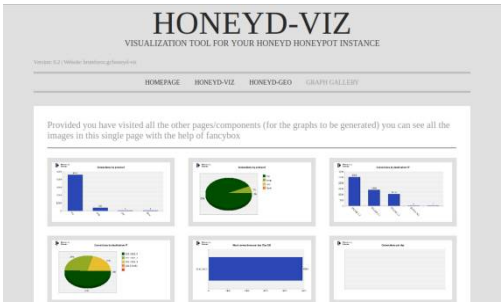
Dari hasil pada gambar diatas serangan *bruteforce* tidak berhasil mendapatkan *password* pada serangan port SSH dengan alamat IP 192.168.1.3.

4.4 Analisa Aktivitas Serangan Dengan Honeyd-Viz

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



Pada gambar diatas terlihat tampilan awal *log web interfaces* menggunakan honeyd-viz 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. Implementasi *Honeyd* mampu menciptakan *virtual server* atau *server* palsu yang membuat penyerang tertarik untuk melakukan serangan terhadap *server* padahal itu hanya informasi palsu sehingga tidak memberikan dampak pada *server* sebenarnya.
2. Dari hasil pengujian terbukti bahwa tidak terjadi serangan pada *server* asli dengan IP Address 192.168.1.1 tetapi serangan terjadi pada 3 *virtual host* yang diciptakan oleh *honeyd* yaitu IP Address 192.168.1.2 sebanyak 28%, 192.168.1.3 sebanyak 51% dan 192.168.1.4 sebanyak 21%.
3. Dengan memanfaatkan sistem *Honeypot* menggunakan *Honeyd*, hasil dari aktivitas serangan jaringan dapat terlihat secara berkala.
4. Dengan melihat analisa grafik,diagram maupun tabel yang diperlihatkan pada *web interfaces* menggunakan honeyd-viz ini bisa memudahkan *administrator* untuk memprediksi dan menganalisa pola serangan dan jenis serangan apa saja yang dilakukan oleh penyerang terhadap sistem.

5.2 Saran

Beberapa saran yang dapat dijadikan pertimbangan dalam mengembangkan penelitian ini adalah :

1. Penambahan aturan pada *honeyd* supaya bisa dikembangkan menjadi *honeynet* .
2. Implementasi honeypot tidak hanya pada jaringan lokal saja melainkan pada jaringan *wireless* maupun jaringan publik
3. Penambahan jumlah penyerang yang lebih dari satu untuk mengetahui seberapa tangguh kinerja dari *honeypot* tersebut.
4. Akan lebih bagus lagi apabila *honeyd* bukan hanya untuk menganalisa aktivitas serangan yang terjadi pada jaringan melainkan diintregasikan dengan IDS agar bisa melakukan *blocking* terhadap serangan yang terjadi pada jaringan.

DAFTAR PUSTAKA

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

Zam, E. (2011) *Buku Sakti Hacker*. Jakarta: Mediakita.

Nurhasanah Umayah, (2012) "*Perancangan dan Implementasi Honeypot pada Virtual Private Server sebagai Penunjang Keamanan Jaringan*", Politeknik Telkom, Bandung

Muhammad Arief (2012). "*Implementasi Honeypot Dengan Menggunakan Dionae di Jaringan Hotspot FIZZ*", Politeknik Telkom, Bandung

Ardianto Setyo Nugroho (2013) "*Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan*", Intitut Sains &Teknologi AKPRIND, Yogyakarta

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

Wikipedia, "*Honeypot (Computing)*" Diakses tanggal 13 Oktober 2014 http://en.wikipedia.org/wiki/Honeypot_(computing)

Niels Provos, "Developments of the Honeyd Virtual Honeypot " Diakses 17 Oktober 2014 http://honeyd.org/

Ulisses Araújo Costa, "*Deploying Honeypots with Honeyd*" Diakses tanggal 17 Oktober 2014 http://ulissesaraujo.wordpress.com/2008/12/08/deploying-honeypots-with-honeyd/