# *Honeypot* Menggunakan *Honeyd* Sebagai Solusi Keamanan Jaringan Dari Aktivitas Serangan

**Nur Fitriana [1], Fata Nidaul Khasanah [1,*]**

[1] Teknik Informatika; STMIK Bina Insani; Jl. Siliwangi No.6 Rawa Panjang Bekasi Bekasi Timur 17114 Indonesia; Telp. (021) 824 36 886 / (021) 824 36 996. Fax. (021) 824 009 24; e-mail: nurfitriana656@gmail.com, fatanidaul@gmail.com

* Korespondensi: e-mail: fatanidaul@gmail.com

Diterima: 19 Oktober 2018; Review: 2 Nopember 2018; Disetujui: 16 Nopember 2018

Cara sitasi: Fitriana N, Khasanah FN. 2018. *Honeypot* Menggunakan *Honeyd* Sebagai Solusi Keamanan Jaringan Dari Aktivitas Serangan. Bina Insani ICT Journal. 5 (2): 143-15.

---

**Abstrak**: Kemudahan dan kecepatan mengirimkan data antar tempat yang berjauhan saat ini telah relatif terpenuhi dengan adanya kemudahan dalam melakukan akses internet. Kemudahan tersebut dikarenakan beberapa institusi telah memiliki arsitektur jaringan komputer masing-masing sehingga memudahkan mereka melakukan akses internet salah satunya sekolahan. Namun sisi lain yang dirasakan ketika pengguna memanfaatkan fasilitas jaringan *wireless* tanpa disadari terdapat suatu ancaman kemanan yang memungkinkan terjadi. Jaringan *wireless* yang berada pada *frekuensi* terbuka seringkali dimanfaatkan oleh *attacker* sebagai jalur masuk untuk menyusup ke jaringan utama. Oleh karena itu diperlukan suatu sistem keamanan yang mampu mendeteksi serangan-serangan yang menuju pada jaringan *wireless*. Salah satu upaya untuk meminimalkan kemungkinan adanya serangan yang terjadi dalam suatu jaringan komputer ketika terkoneksi internet yaitu dengan menambahkan suatu infrastruktur yang nantinya mampu meningkatkan keamanan jaringan. Salah satu teknik yang digunakan untuk memberikan proteksi keamanan jaringan yaitu dengan membangun infrastruktur *honeypot* dengan menggunakan *honeyd*. Hasil penelitian yang telah dilakukan menunjukkan bahwa hasil implementasi *honeypot* menggunakan *honeyd* telah berhasil dilakukan implementasi dan konfigurasi. Beberapa jenis serangan yang dilakukan pengujian diantaranya *Denial of Service attack, File Transfer Protocol attack, Internet Control Message Protocol* dan *scan attack*. Dari ketiga jenis serangan tersebut dilakukan pengujian dilanjutkan dengan pengamatan. Pengamatan dilihat dari segi waktu yang dibutuhkan oleh *honeyd* berhasil menampilkan notifikasi di *log honeyd* ketika serangan masuk. Berdasarkan hasil pengamatan diperoleh rata-rata waktu yang diperlukan untuk jenis serangan *DoS* 2,33 detik, serangan *FTP* 2 detik dan serangan *ICMP* 5 detik.

**Kata kunci:** *DoS attack, FTP attack, Honeypot, Honeyd, ICMP*, Keamanan Jaringan

***Abstract:*** *The ease and speed of sending data between places that currently have relatively far apart are met with the ease of access to the internet. Due to the ease of some institutions already have a computer network architecture each so they do make it easier to access the internet one schoolgirl. But the other side felt when users utilize the wireless network facilities there unwittingly a security threat that allow to happen. The wireless network is an open frequency often exploited by the attacker as the incoming line to creep into the main network. Therefore required a security system capable of detecting these attacks led to the wireless network. One of the efforts to minimize the possibility of an attack happening in a computer network when connected to the internet by adding an infrastructure that was later able to improve network security. One of the techniques used to provide network security protection that is by building the infrastructure using the honeypot honeyd. The results of the research that has been done shows that the results of the implementations use honeyd honeypot has successfully performed the implementation and configuration. Some types of attacks conducted testing include Denial of Service attack, File Transfer Protocol attack, Internet Control Message*

*Copyright@2018. P2M STMIK BINA INSANI*

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 143 - 152

*Protocol and the scan attack. Of the three types of such attacks carried out testing followed by observation. The observations seen in terms of the time required by the notification on successful honeyd log incoming attack honeyd. Based on the observations obtained the average time required for this type of DoS attack 2.33 seconds, FTP attacks attacks ICMP 2 seconds and 5 seconds.*

***Keywords**: DoS attack, FTP attack, Honeypot, Honeyd, ICMP, Network Security*

## 1. Pendahuluan

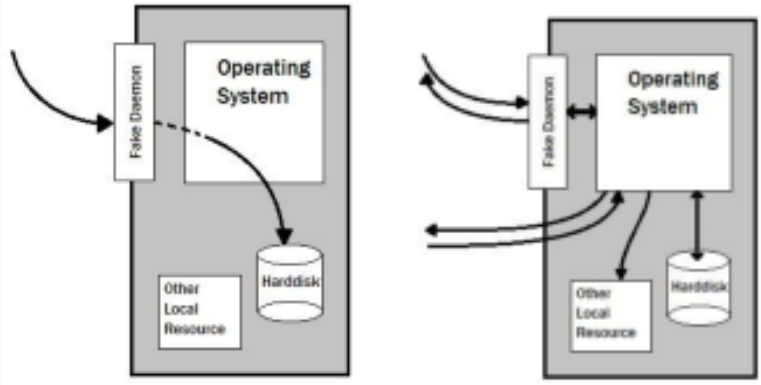
Pada zaman sekarang kemudahan dan kecepatan mengirimkan data antar tempat yang berjauhan telah relatif terpenuhi, ketakutan mulai muncul dari pihak pengguna layanan internet. Jaringan komputer telah menjadi media pertukaran informasi antar belahan dunia tetapi tidak semua informasi bersifat terbuka untuk umum. Pihak-pihak yang terhubung ke internet tidak semuanya berkarakter baik dan sopan, sejumlah pengguna internet memiliki motivasi pribadi untuk sekedar usil ataupun bahkan berusaha menembus sistem keamanan hingga akhirnya dapat menimbulkan kerugian baik finansial maupun sumber daya lainnya hingga dapat menimbulkan kekacauan sistem. Untuk itu sesaat setelah komputer terkoneksi dengan internet saat ini menjadi perhatian khusus.

Beberapa sekolahan saat ini telah mengimplementasikan jaringan komputer untuk terhubung ke internet. Fasilitas tersebut dapat dirasakan oleh para guru dan juga murid, yang secara tidak langsung memberikan kemudahan dan manfaat baik dalam proses akademik maupun non-akademik. Dari sisi lain, selain manfaat dan kemudahan yang didapat ketika pengguna memanfaatkan fasilitas jaringan *wireless* tanpa disadari terdapat suatu ancaman kemanan yang memungkinkan terjadi. Jaringan *wireless* yang berada pada *frekuensi* terbuka seringkali dimanfaatkan oleh *attacker* sebagai jalur masuk untuk menyusup ke jaringan utama. Oleh karena itu diperlukan suatu sistem keamanan yang mampu mendeteksi serangan-serangan yang menuju pada jaringan *wireless*.

Salah satu upaya untuk meminimalkan kemungkinan adanya serangan yang terjadi dalam suatu jaringan komputer ketika terkoneksi internet yaitu dengan menambahkan suatu infrastruktur yang nantinya mampu meningkatkan keamanan jaringan. Salah satu teknik yang digunakan untuk memberikan proteksi keamanan jaringan yaitu dengan membangun infrastruktur *honeypot* dengan menggunakan *honeyd*.

*Honeypot* merupakan sistem yang memiliki konsep kerja yang menyerupai sistem asli. Hal tersebut bertujuan untuk mengamankan sistem asli agar tidak diserang maupun disusupi oleh penyerang. Jadi apabila terjadi serangan terhadap suatu sistem asli maka serangan tersebut akan dialihkan, sehingga sistem yang asli tetap aman dan terhindar dari serangan [Cahyanto et al., 2013].

*Honeypot* juga dapat dimanfaatkan untuk memperoleh informasi penting dari kegiatan yang dilakukan oleh penyerang. Selain itu dengan adanya *honeypot* admin juga dapat mempelajari pola atau metode yang digunakan untuk menyerang sistem yang nantinya dapat solusi pencegahan yang lebih baik dari pola penyerang [Aidin et al., 2016].




Sumber: [Aidin et al., 2016]

Gambar 1. *Low Interaction Honeypot* dan *High Interaction Honeypot*

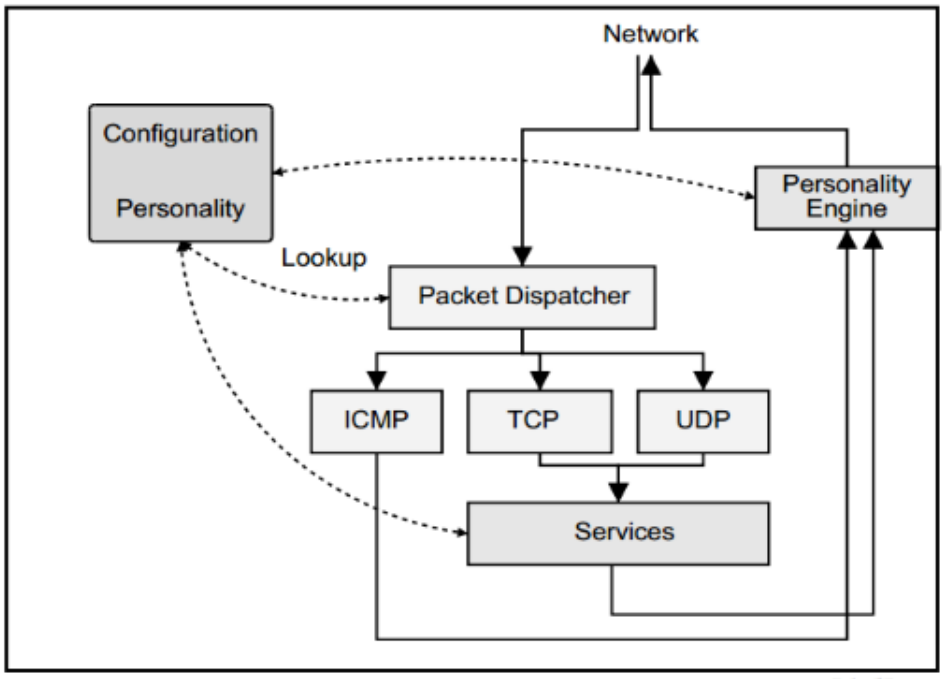
Terdapat dua jenis *honeypot*, yaitu *low interaction honeypot* dan *high interaction honeypot*. *Low interaction honeypot* merupakan jenis *honeypot* yang memiliki karakteristik lebih mudah dan cepat untuk diterapkan, hal tersebut dikarenakan *honeypot* jenis ini hanya menyediakan tiruan dari layanan tertentu saja. Dan *honeypot* jenis *low interaction* tidak terdapat sistem operasi nyata yang dimanfaatkan sebagai tempat operasi penyerangan. *High interaction honeypot* merupakan jenis *honeypot* yang memberikan sistem dan layanan nyata layaknya sistem yang sesungguhnya, oleh karena itu penyerang dapat melakukan kontrol penuh pada sistem *honeypot* [Aidin et al., 2016].

*Honeyd* merupakan suatu program komputer yang bersifat *open source*. Cara kerja *honeyd* memungkinkan pengguna untuk membuat dan menjalankan beberapa *virtual host* dalam jaringan komputer. Dari *virtual host* tersebut pengguna dapat mensimulasikan suatu konfigurasi jaringan komputer untuk meniru beberapa jenis server [Aidin et al., 2016].

Tujuan dari penelitian ini adalah mengimplementasikan *honeypot* menggunakan *honeyd* yang dijadikan sebagai solusi untuk memberikan kemanan jaringan *wireless* terhadap aktivitas serangan. Beberapa jenis serangan yang dilakukan pengujian diantaranya serangan *Denial of Service (DoS)*, *File Transfer Protocol (FTP)* dan *Internet Control Message Protocol (ICMP)*. Dengan adanya *honeypot honeyd* diharapkan kemungkinan upaya-upaya penyerangan yang dilakukan oleh penyerang dapat diatasi dan terdapat pemberitahuan melalui *log honeyd.*

## 2. Metode Penelitian

*Honeyd* memiliki arsitektur proses dimana ketika paket tiba maka *dispatcher* akan merespon paket yang diminta. Kemudian paket akan diproses oleh *personality engine*, hal tersebut bertujuan untuk menyesuaikan isi paket, sehingga paket tampak berasala dari server sesungguhnya. Tiga protokol yang dapat diketahui oleh *honeypot honeyd* adalah *Internet Control Message Protocol (*ICMP), *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).

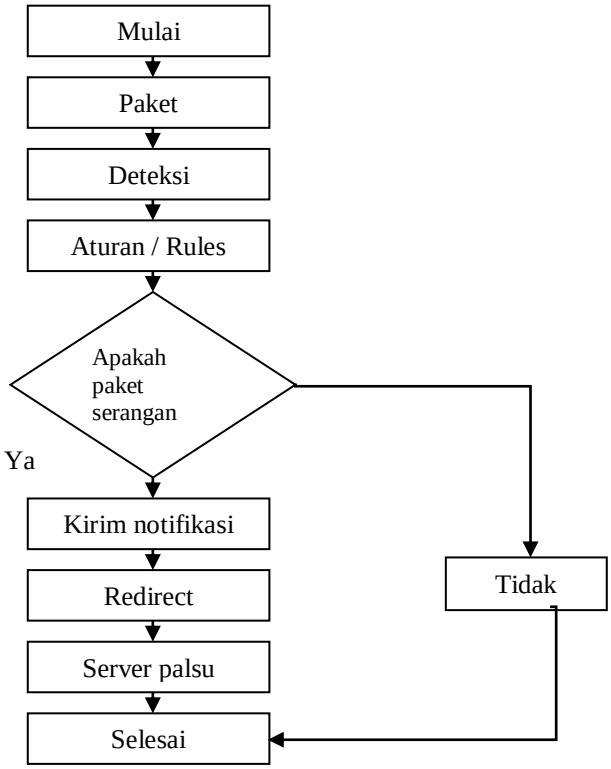



Sumber: [Utdirartatmo, 2005]

Gambar 3. Arsitektur *Honeyd*

Diagram alir untuk pencegahan penyusupan dimulai ketika terdapat paket data masuk maka paket tersebut akan dilakukan pengecekan atau proses pendeteksian. Kemudian dilanjutkan dengan pembandingan apakah paket yang masuk sesuai dengan *rules* yang telah dibuat. Jika terjadi serangan maka akan terdapat notifikasi atau *alert* kemudian akan dibelokkan serangan tersebut ke *Honeyd*. Dan apabila paket tersebut bukan serangan maka paket data akan dikirim ke server.

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 143 - 152




Sumber: Hasil Penelitian (2017)

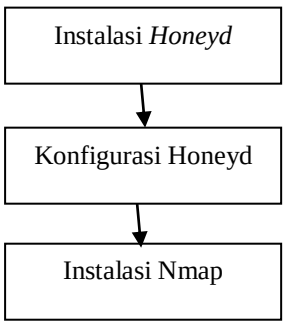
Gambar 4. *Flowchart* Pencegahan Penyusupan

## 3. Hasil dan Pembahasan

Pada pembahasan hasil pembahasan akan dibahas mengenai hasil implementasi *honeypot honeyd* dan hasil pengujian dari beberapa jenis serangan.

### 3.1 Hasil Instalasi

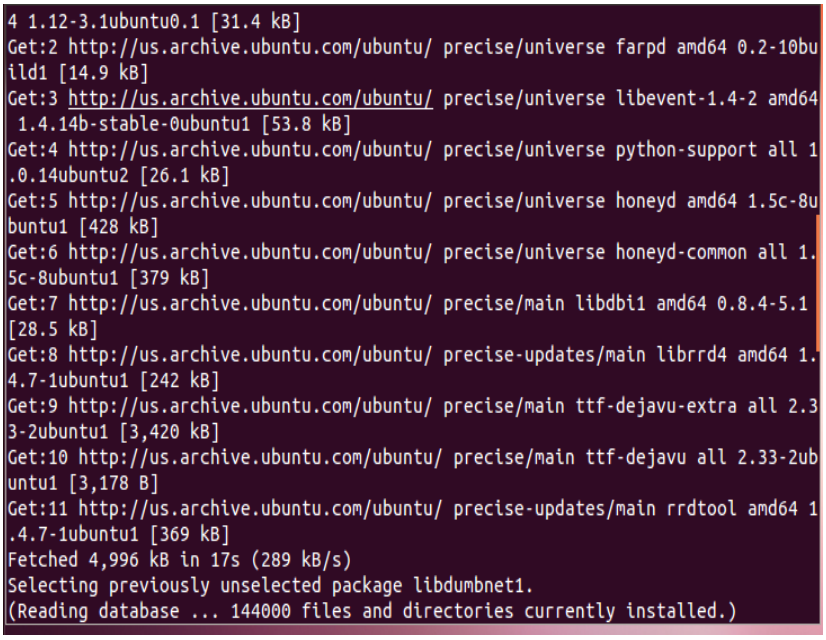
Implementasi *honeypot* menggunakan *honeyd* dilakukan dengan menggunakan sistem operasi Ubuntu 12.04 LTS. Terdapat tiga perangkat lunak yang perlu diinstal dalam Ubuntu 12.04 LTS, yaitu instalasi *honeypot,* instalasi *honeyd* dan instalasi *nmap.*




Sumber: Hasil Penelitian (2017)

Gambar 5. Alur Instalasi *Honeyd*

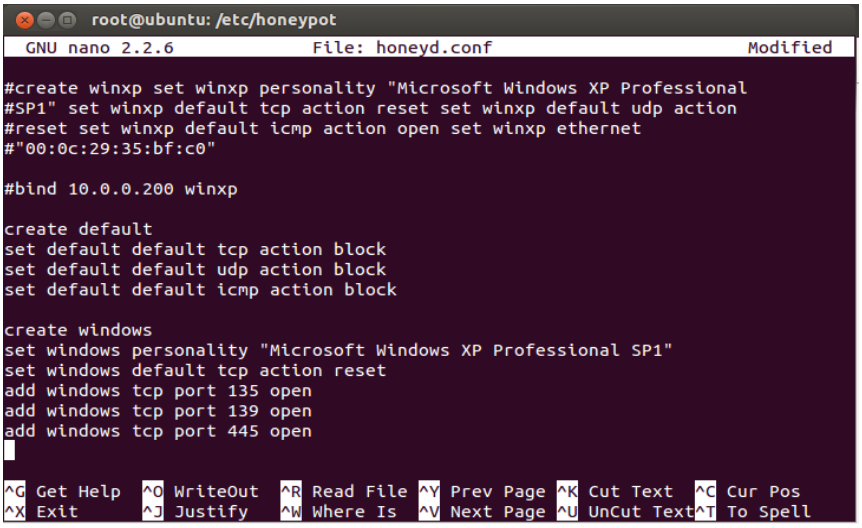
Tahap awal instalasi *honeyd* di *honeypot* dengan mengetahui lokasi file *honeypot*, kemudian proses instalasi dilakukan dengan format *apt-get install honeyd*. Setalah proses instalasi berhasil maka dilanjutkan dengan proses konfigurasi *honeyd.*




Sumber: Hasil Penelitian (2017)

Gambar 6. Hasil Instalasi *Honeyd*

Konfigurasi *honeyd* akan mendefinisikan beberapa hal, yang pertama adalah *personality* yang berarti ketika *device* lain terkoneksi dengan *honeypot* ini maka *honeypot* ini akan dikenali sebagai windows XP SP1. Pada *template windows* ini juga akan dibuka tiga *ports* yaitu 135,139 dan 445. Ini merupakan *ports* yang biasa dipakai pada *windows system* "*action resert*" adalah akan menghentikan *traffic* yang tidak termasuk open ports yang didefinisikan pada file konfigurasi "set windows *ethernet*" akan mengeset *MAC address* untuk *honeypot*, hal ini dibutuhkan jika menjalankan *honeyot* dengan DHCP.

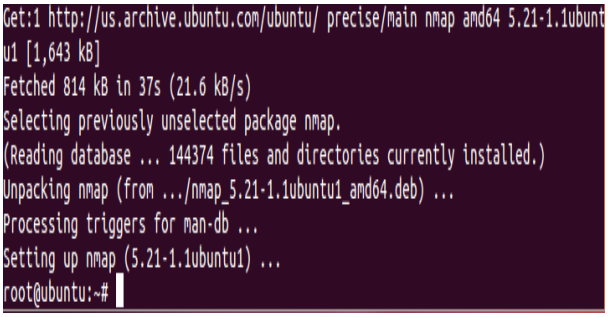



Sumber: Hasil Penelitian (2017)

Gambar 7. Hasil Konfigurasi *Honeyd*

Setelah melakukan instalasi *honeyd* dan konfigurasi *honeyd* maka proses selanjutnya melakukan instalasi *nmap. Nmap* berfungsi untuk melakukan *scanning* aktifitas-aktifitas penyerang yang mencoba untuk melakukan penyerangan.

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 143 - 152



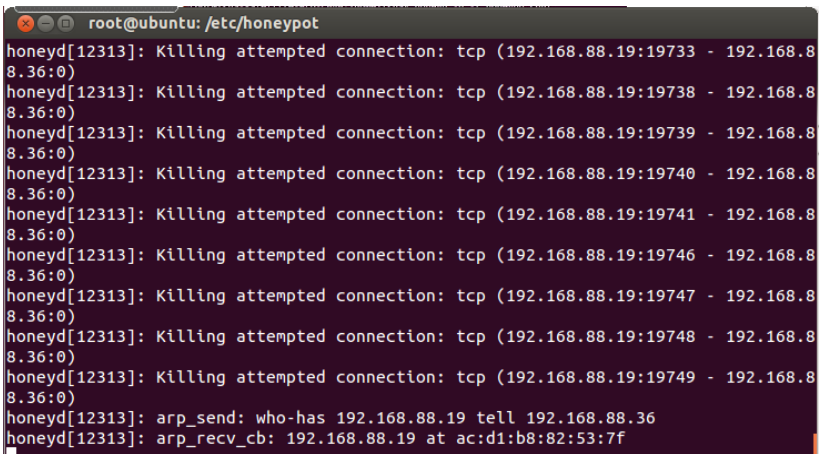

Sumber: Hasil Penelitian (2017)

Gambar 8. Hasil Instalasi *Nmap*

### 3.2 Hasil Pengujian

Setelah proses instalasi dan konfigurasi *hoenyd* berhasil, selanjutnya dilanjutkan dengan proses pengujian terhadap beberapa jenis serangan. Beberapa jenis serangan yang dilakukan pengujian diantaranya *DoS attack*, *FTP attack* dan *ICMP*.

*Denial of Service* merupakan suatu aktifitas yang menghambat sebuah layanan bahkan mematikan layanan sehingga *user* yang memiliki otorisasi tidak dapat menggunakan layanan. Beberapa cara yang dilakukan oleh penyerang dalam melakukan serangan *DoS* diantaranya penyerang mencoba untuk membanjiri (*flood*) jaringan dengan demikian dapat mencegah lalu lintasi yang *legal* pada jaringan, penyerang mencoba mengganggun koneksi antara dua mesin sehingga dapat mencegah akses layanan, penyerang mencoba untuk mencegah individu tertentu ketika mengakses layanan, penyerang mencoba mengganggu layanan sistem yang spesifik [Sumarno and Bisoro, 2003]. Pada proses pengujian serangan kali ini dilakukan oleh *attacker* yaitu dengan cara memasukkan perintah *nmap* diikuti dengan alamat IP sasaran, kemudian *attacker* akan mengetahui IP yang aktif. Setelah mengetahui IP aktif *attacker* melakukan serangan dengan mengetikkan perintah ping terhadap IP yang aktif. Hasil serangan yang dilakukan attacker ke IP sasaran yang telah memiliki keamanan *honeyd* menunjukkan bahwa *attacker* tidak dapat memperoleh data yang ditunjukkan dengan adanya tulisan *packet loss*. Kemudian dari sisi notifikasi *honeyd* akan menampilkan IP penyerang dengan cara menghabiskan sumber atau *resource* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.




Sumber: Hasil Penelitian (2017)

Gambar 9. Hasil *DoS Attack*

Selanjutnya dilakukan pengamatan terhadap notifikasi ketika ada serangan *DoS* terjadi. Pengamatan dilihat dari segi waktu yang dibutuhkan oleh terminal *honeyd* atau *log honeyd* berhasil menampilkan notifikasi serangan *DoS*. Dalam tabel tersebut menunjukkan bahwa rata-

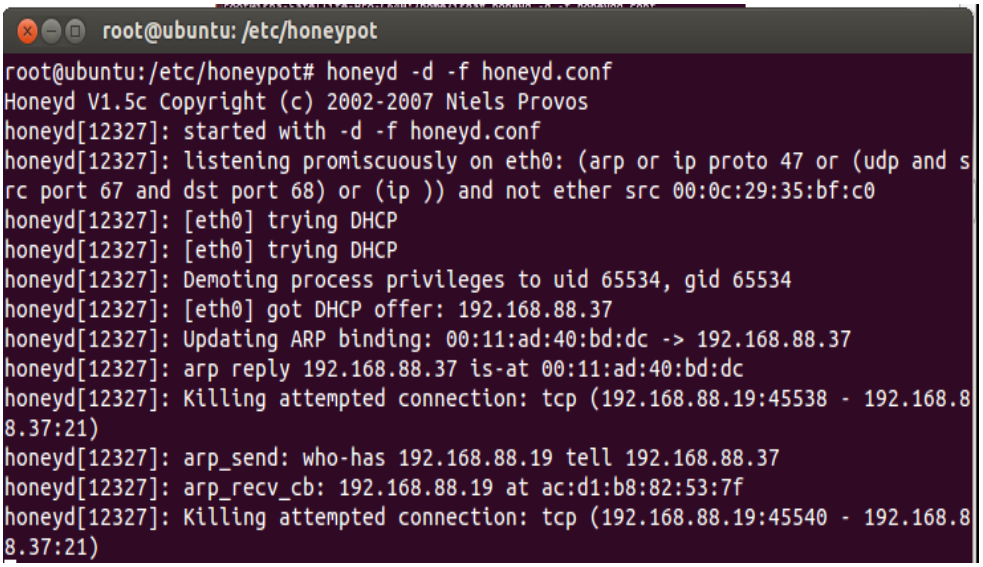
rata waktu yang dibutuhkan oleh *honeyd* untuk memunculkan notifikasi ketika serangan masuk adalah 2,33 detik dengan tiga kali percobaan.

Tabel 1. Tabel Hasil Pengujian *DoS*

| Pengujian ke | *IP Adreess* | Waktu (detik) |
|---|---|---|
| 1 | 191.168.88.27 | 2 |
| 2 | 192.168.88.27 | 3 |
| 3 | 192.168.88.27 | 2 |
| Rata-Rata Waktu | | 2,33 |

Sumber: Hasil Penelitian (2017)

*File Transfer Protocol* (FTP) adalah serangan *buffer overflow* yang diakibatkan oleh perintah *malformed*. Tujuan menyerang FTP server ini rata-rata adalah untuk mendapatkan command shell ataupun unutuk melakukan *Denial Of Service*. Serangan *Denial Of Service* akhirnya dapat menyebabkan seorang *user* atau *attacker* untuk mengambil *resource* didalam jaringan tanpa adanya autorisasi, sedangakan *command shell* dapat membuat seorang *attacker* mendaptakan akses ke sistem server dan file data akhirnya seorang *attacker* bisa membuat *anonymous foot-access* yang mempunyai hak penuh terhadap sistem bahkan jaringan yang diserang.




Sumber: Hasil Penelitian (2017)

Gambar 10. Hasil *FTP Attack*

Selanjutnya dilakukan pengamatan terhadap hasil pengujian jenis serangan *FTP attack*. Hasil tersebut diperoleh dengan melakukan pengamatan waktu yang dibutuhkan oleh terminal *honeyd* berhasil menampilkan notifikasi serangan *FTP attack*. Dalam tabel tersebut menunjukkan bahwa rata-rata waktu yang dibutuhkan oleh *honeyd* untuk memunculkan notifikasi di *log honeyd* ketika serangan masuk adalah 2 detik dari tiga kali percobaan.

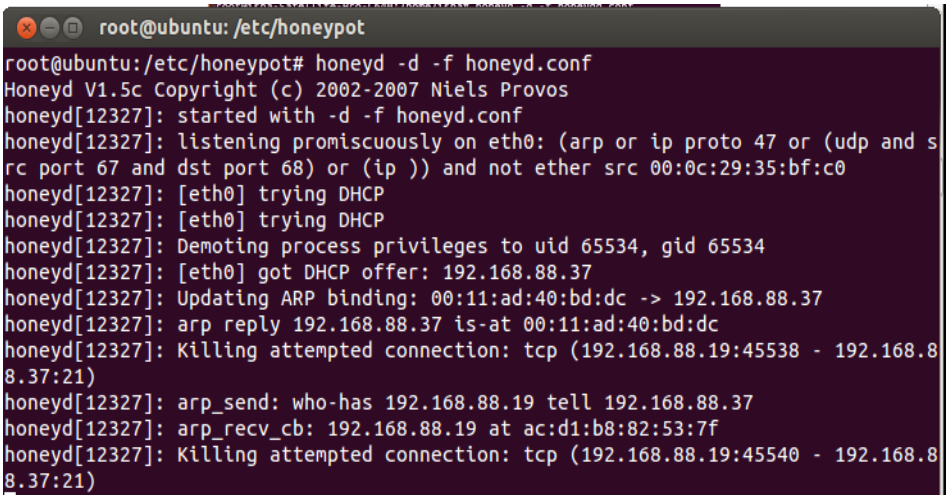
ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 143 - 152

Tabel 2. Tabel Pengujian *FTP Attack*

| Pengujian ke | *IP Address* | Waktu (detik) |
|---|---|---|
| 1 | 191.168.88.38 | 1 |
| 2 | 192.168.88.38 | 2 |
| 3 | 192.168.88.38 | 3 |
| Rata-Rata Waktu | | 2 |

Sumber: Hasil Penelitian (2017)

Serangan *Internet Control Message Protocol (ICMP)* adalah jenis serangan yang membanjiri koneksi jaringan lokal dengan mengirimkan serangkaian permintaan *echo* ke server. Kemudian server melalui *honeyd* mengirimkan jumlah *exceesive* untuk merespon serangan yang masuk dengan mengirimkan banyak *byte*, namun serangan itu mungkin tidak memiliki *destiantion routatble* karena alamat IP yang digunakan palsu.



Sumber: Hasil Penelitian (2017)

Gambar 11. Hasil Serangan ICMP

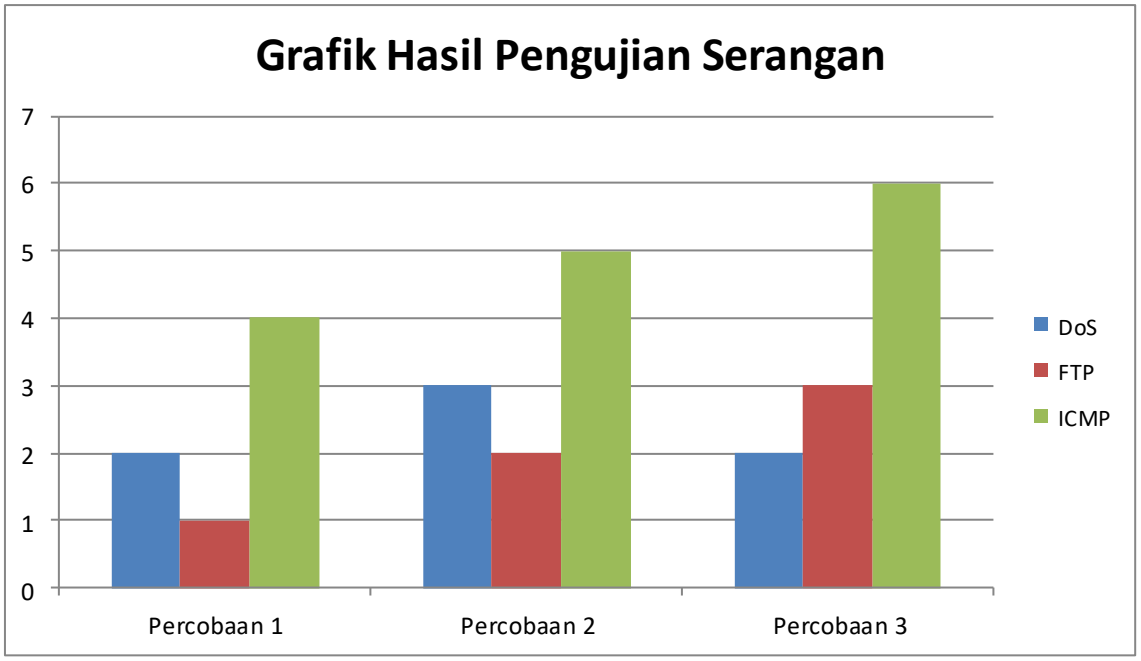
Hasil pengujian jenis serangan ICMP diperoleh dengan melakukan pengamatan waktu yang dibutuhkan oleh terminal *honeyd* berhasil menampilkan notifikasi serangan ICMP. Dalam tabel tersebut menunjukkan bahwa rata-rata waktu yang dibutuhkan oleh *honeyd* untuk memunculkan notifikasi di *log honeyd* ketika serangan masuk adalah 5 detik dari tiga kali percobaan.

Tabel 3. Tabel Pengujian ICMP

| Pengujian ke | *IP Address* | Waktu (detik) |
|---|---|---|
| 1 | 192.168.88.41 | 4 |
| 2 | 192.168.88.41 | 5 |
| 3 | 192.168.88.41 | 6 |
| Rata-Rata Waktu | | 5 |

Sumber: Hasil Penelitian (2017)

Dari ketiga pengujian terhadap serangan DoS, FTP dan ICMP dibuat grafik hasil pengamatan terhadap ketiga jenis serangan sampai muncul notifikasi bahwa telah terjadi serangan yang masuk di *log honeyd*. Pengamatan waktu diperoleh dari tiga kali pengujian terhadap masing-masing jenis serangan.




Sumber: Hasil Penelitian (2017)

Gambar 12. Grafik Hasil Pengujian Serangan

## 4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan menunjukkan bahwa hasil implementasi *honeypot* menggunakan *honeyd* telah berhasil dilakukan implementasi dan konfigurasi. Dengan adanya *honeypot honeyd* yang terpasang maka dapat dijadikan solusi untuk memberikan keamanan jaringan *wireless* terhadap kemungkinan serangan-serangan yang terjadi dapat teratasi. Beberapa jenis serangan yang dilakukan pengujian diantaranya *Denial of Service attack, File Transfer Protocol attack, Internet Control Message Protocol* dan *scan attack*. Dari ketiga jenis serangan tersebut dilakukan pengujian dilanjutkan dengan pengamatan. Pengamatan dilihat dari segi waktu yang dibutuhkan oleh *honeyd* berhasil menampilkan notifikasi di *log honeyd* ketika serangan masuk. Berdasarkan hasil pengamatan diperoleh rata-rata waktu yang diperlukan untuk jenis serangan *DoS* 2,33 detik, serangan *FTP* 2 detik dan serangan *ICMP* 5 detik.

## Referensi

Aidin LP, Nasution SM, Azmi F. 2016. Implementasi High Interaction Honeypot Pada Server. In: e-Proceeding of Engineering., p 2172–2178.

Cahyanto TA, Oktavianto H, Royan AW. 2013. Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan. JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones. 1: 86–92.

Komputer W. 2014. Konsep dan Implementasi Jaringan dengan Linux Ubuntu. Yogyakarta: Andi Offset.

Sofana I. 2017. Jaringan Komputer Berbasis Mikrotik. Bandung: Informatika.

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 143 - 152

Sumarno, Bisoro S. 2003. Solusi Network Security Dari Ancaman SQL Injection Dan Denial of Service ( Dos ). Teknolojia 5: 19–30.

Utdirartatmo F. 2005. Trik Menjebak Hacker dengan Honeypot. Yogyakarta: Andi Offset.