Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless

Bagus Mardiyanto[1], Tutuk Indriyani[2], I Made Suartana[3]
[1,2]Teknik Informatika – Institut Teknologi Adhi Tama Surabaya
[3]Teknik Informatika, Universitas Negeri Surabaya
Email: Diandradns@gmail.com

Abstract *The development of network technology, especially networking security system, demands the security system to evolve. Honeyd is honeypot with low interaction type which has smaller risk than high interaction type. It is because the interaction to honeypot does not directly engage with the real system. In this research, honeyd is integrated with iptables implemented to local network by trying several attacks, such as scanning host, DoS, and Ddos. From the result of honeyd log, the gained information data is processed with honeyd-viz and is expected to become an inputand solution to decide the security policy in network and make the system safer. The experiment showed that honeyd was able to detect the attack by Netscan android by doing scanning host in network. In Ddos attack experiment using Loic, average cpu load before the attack was 15.25%, while after the attack cpu load was 45.98%, and after attack deflection the cpu load was 30.83%.*

Keywords: *Honeypot, Honeyd, Honeyd-viz, Iptables, Dos, Ddos, Netscan.*

Abstrak Perkembangan teknologi jaringan terutama sistem keamanan jaringan yang semakin berkembang menuntut agar sistem keamanan untuk berkembang. *Honeyd* merupakan *honeypot* dengan jenis *low interaction* yang memiliki resiko jauh lebih kecil dibandingkan dengan jenis *high interaction* karena interaksi terhadap *honeypot* tidak langsung melibatkan sistem yang sesungguhnya. Pada penelitian ini, honeyd yang dipadu dengan iptables diimplementasikan pada jaringan lokal dengan mencoba beberapa serangan seperti *scanning host*, *DoS* dan *Ddos.* Dari hasil log honeyd data informasi yang didapat diolah dengan honeyd-viz dan diharapkan dapat menjadi masukan dan solusi untuk menentukan kebijakan keamanan pada jaringan dan membuat sistem lebih aman. Dalam percobaan yang dilakukan honeyd dapat mendeteksi serangan yang dilakukan oleh Netscan android dalam scanning host pada jaringan. Pada percobaan serangan Ddos dengan Loic didapatkan nilai rata-rata sebelum serangan beban cpu sebesar 15,25% dan setelah serangan beban cpu sebesar 45,98% dan setelah pembelokkan serangan beban cpu sebesar 30,83%.

Kata kunci: *Honeypot, Honeyd, Honeyd-viz, Iptables, Dos, Ddos,, Netscan.*

1. Pendahuluan

Keamanan jaringan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Teknologi sistem keamanan konvensional seperti *firewall* dan *IDS* (*Intrusion Detection System*) memang cukup baik, hanya saja masih memiliki beberapa kelemahan. Kebanyakan IDS sulit membedakan antara aktivitas legal dengan trafik malicious. Misal kalau ada posting dari BugTraq tentang bahaya suatu kode *exploit*, maka bisa saja dianggap oleh IDS sebagai *buffer overflow*, karena polanya cocok.

Serangan yang paling sering digunakan adalah *Port Scanning* dan DOS (Denial Of Service). *Port Scanning* adalah serangan yang bekerja untuk mencari port yang terbuka pada suatu jaringan komputer, dari hasil port scanning akan di dapat letak kelemahan sistem jaringan komputer tersebut. DOS adalah serangan yang bekerja dengan cara mengirimkan request ke server berulang kali untuk bertujuan membuat server menjadi sibuk menanggapi request dan server akan mengalami kerusakan atau hang (Renuka P, Dr Annamma, Suhas.V, Kundan Kumar, 2010).

Menurut beberapa sumber honeypot adalah sistem keamanan yang fungsinya untuk diselidiki, diserang, atau dikompromikan. (Addison Wesley, 2002). Pada umumnya honeypot berupa komputer, data, atau situs jaringan yang terlihat seperti bagian dari jaringan, tapi sebenarnya terisolasi dan dimonitor. Jika dilihat dari kacamata hacker yang akan menyerang, honeypot terlihat seperti layaknya sistem yang patut untuk diserang. (wilvan aneldi, 2012).

Hingga saat ini serangan *Distributed Denial of Service* (Ddos) yang dilakukan oleh *attacker* pada server dan layanan Internet masih menggunakan komputer sebagai media penyerangan. Dengan semakin majunya teknologi *mobile* kita bisa menggunakan *smartphone* android untuk melakukan serangan *Distributed Denial of Service* (Ddos) pada server dan layanan internet menggunakan sebuah *tools.*

2. Tinjauan Pustaka

2.1. Honeypot

Honeypot adalah *security resource* yang yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan (Firrar Utdirartatmo, 2005:1). Pada umumnya Honeypot berupa komputer, data, atau situs jaringan yang terlihat seperti bagian dari jaringan, tapi sebenarnya terisolasi dan dimonitor. Jika dilihat dari kacamata hacker yang akan menyerang, Honeypot terlihat seperti layaknya sistem yang patut untuk diserang.

2.2. Honeyd

Honeyd adalah open source program komputer yang dibuat oleh Niels Provos yang memungkinkan pengguna untuk membuat dan menjalankan beberapa virtual host pada jaringan komputer. Host virtual ini dapat dikonfigurasi untuk meniru beberapa jenis server yang memungkinkan pengguna untuk mensimulasikan jumlah tak terbatas konfigurasi jaringan komputer. Honeyd digunakan terutama dalam bidang keamanan komputer .

Honeyd digunakan terutama untuk dua tujuan. Menggunakan kemampuan perangkat lunak untuk meniru banyak host jaringan yang berbeda sekaligus (hingga 65536 host sekaligus), Honeyd dapat bertindak sebagai gangguan potensi hacker . Jika jaringan hanya memiliki 3 server yang nyata, tetapi satu server menjalankan Honeyd, jaringan akan muncul menjalankan ratusan server untuk hacker. Hacker kemudian akan harus melakukan penelitian lebih lanjut (mungkin melalui rekayasa sosial) untuk menentukan server adalah nyata, atau hacker mungkin terjebak dalam honeypot.

2.3. Iptables

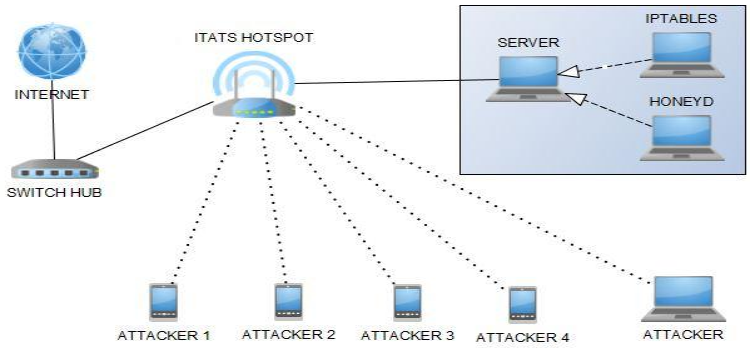
Iptables merupakan utility firewall powerfull yang banyak digunakan. Iptables adalah pengganti ipchains dan mendukung kernel 2.4 serta memiliki fitur yang banyak dibanding ipchain, diantaranya : (a) Connections tracking capability : misalnya kemampuan untuk inpeksi paket serta bekerja dengsn icmp dan udp sebagaimana koneksi tcp. (b) Menyederhanakan perilaku paket-paket dalam melakukan negoisasi built in chain (input, output dan forward). (c)

Rate-limited connection dan logging capability. Kita dapat membatasi usaha-usaha koneksi sebagai tindakan preventif serangan Syn flood denial of services (DOS).

3. METODE PENELITIAN

3.1. Gambaran Umum Sistem

Dalam perancangan analisa dan implementasi honeyd dalam mendeteksi serangan ddos pada jaringan wireless, penulis ingin menganalisa beberapa parameter meliputi *denial of service,* trafik jaringan. Dari analisa tersebut dapat diketahui permasalahan dan cara untuk mengatasi permasalahan keamanan jaringan komputer.

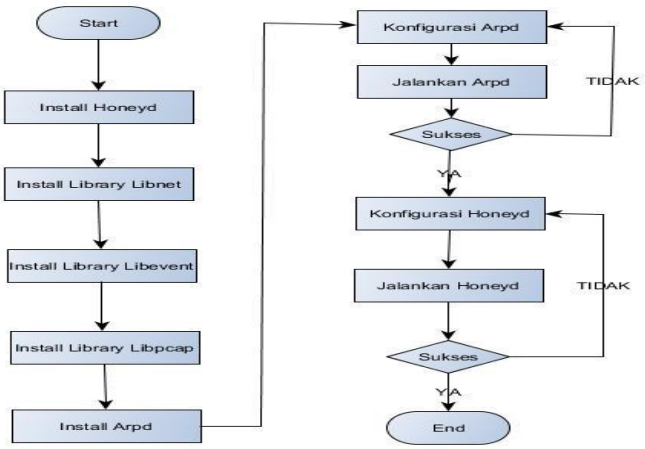


Gambar 1. Arsitektur Jaringan

3.2. Rancangan Honeypot

Rancangan sistem Honeypot dalam penelitian ini memakai jenis Honeypot yaitu Honeyd. Honeyd yang telah dikonfigurasi digunakan untuk membuat dan menjalankan virtual host dalam jaringan komputer dan mendeteksi serangan-serangan yang dilakukan oleh Attacker. Pada Honeyd terdapat file konfigurasi yaitu Honeyd.conf didalamnya terdapat beberapa konfigurasi diantaranya adalah *personality. Personality* sendiri merupakan sebuah konfigurasi yang digunakan untuk membuat Honeyd meniru/menyamar sebagai sistem operasi tertentu.

Dengan adanya konfigurasi *personality* tersebut ketika ada device lain terkoneksi dengan jaringan yang sama maka Honeyd akan dikenali, Seperti Port-port yang telah dibuka dan juga jenis protokol-protokol yang di ijinkan dan yang akan diblokir. Bind berfungsi untuk pemberian IP setiap virtual Honeyd yang telah dibuat. Berikut ini adalah diagram alur rancangan implementasi Honeyd :



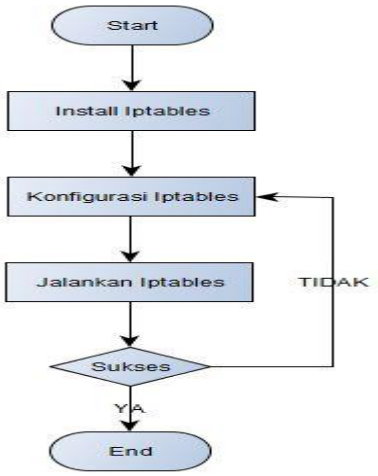
Gambar 2. Flowchart implementasi honeyd

Pada flowchart diatas secara sederhana menjelaskan bahwa terlebih dahulu menginstall honeyd dan kemudian library-library yang dibutuhkan diantaranya adalah library libdnet, library

libevent, dan arpd. Setelah semua itu terinstall barulah mengkonfigurasi arpd dan menjalankannya. Jika proses konfigurasi dan menjalankannya menemukan kendala maka akan kembali lagi ke proses konfigurasi arpd, dan jika sukses maka ke proses selanjutnya yaitu konfigurasi honeyd dan menjalankan honeyd. Ketika menjalankan honeyd menemukan kendala maka akan kembali lagi ke proses konfigurasi honeyd dan jika sukses maka konfigurasi telah selesai dan Honeyd dapat digunakan.

3.3. Rancangan Iptables

Rancangan firewall yaitu iptables yang secara default telah ada dalam Ubuntu. Rancangan sistem iptables yang telah dikonfigurasi digunakan untuk melindungi dan memblok serangan yang terjadi pada server.



Gambar 3. Flowchart implementasi Iptables

Pada flowchart diatas secara sederhana menjelaskan bahwa terlebih dahulu menginstall iptables. Setelah terinstall barulah mengkonfigurasi iptables dan menjalankannya. Jika proses konfigurasi dan menjalankannya menemukan kendala maka akan kembali lagi ke proses konfigurasi iptables jika sukses maka konfigurasi telah selesai dan iptables dapat digunakan.

3.4. Skenario Serangan

Skenario uji coba yang akan dilakukan adalah sebagai berikut :

1. Host scanning dan port scanning

   Pengujian pertama yang dilakukan adalah host scanning dan port, yang bertujuan untuk mengetahui host yang sedang aktif dan port yang sedang terbuka. Hal ini juga bertujuan untuk membuktikan serangan attacker dan sistem honeyd yang telah dibuat berjalan dengan benar.
2. Serangan Ddos TCP Flood

   Skenario DDOS attack ini ditujukan ke honeyd yang telah dibuat. Pada skenario ini hacker melakukan penyerangan DDOS (Distributed Denial of Service) pada honeyd menggunakan tools loic dengan jenis serangan TCP Flood.
3. Serangan Ddos HTTP Flood

   Skenario DDOS attack ini ditujukan ke honeyd yang telah dibuat. Pada skenario ini hacker melakukan penyerangan DDOS (Distributed Denial of Service) pada honeyd menggunakan tools loic dengan jenis serangan Http Flood.
4. Serangan Ddos UDP Flood

   Skenario DDOS attack ini ditujukan ke honeyd yang telah dibuat. Pada skenario ini hacker melakukan penyerangan DDOS (Distributed Denial of Service) pada honeyd menggunakan tools loic dengan jenis serangan UDP Flood
5. Serangan Ddos ke Server sebelum konfigurasi iptables

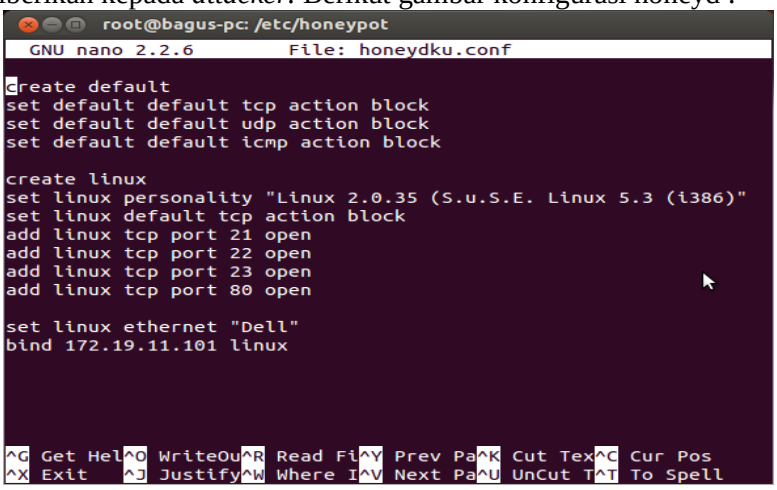
Skenario DDOS attack ini ditujukan ke server yang telah dibuat dan iptables belum dijalankan. Pada skenario ini hacker melakukan penyerangan DDOS (Distributed Denial of Service) pada server menggunakan tools loic dengan jenis serangan Tcp Flood.

6. Serangan Ddos ke Server setelah konfigurasi iptables

Skenario DDOS attack ini ditujukan ke server yang telah dibuat dan iptables telah dijalankan. Pada skenario ini hacker melakukan penyerangan DDOS (Distributed Denial of Service) pada server menggunakan tools loic dengan jenis serangan Tcp Flood.

4. HASIL DAN PEMBAHASAN

Konfigurasi honeyd digunakan untuk tujuan membuat sistem operasi palsu beserta layanan yang diberikan kepada *attacker*. Berikut gambar konfigurasi honeyd :



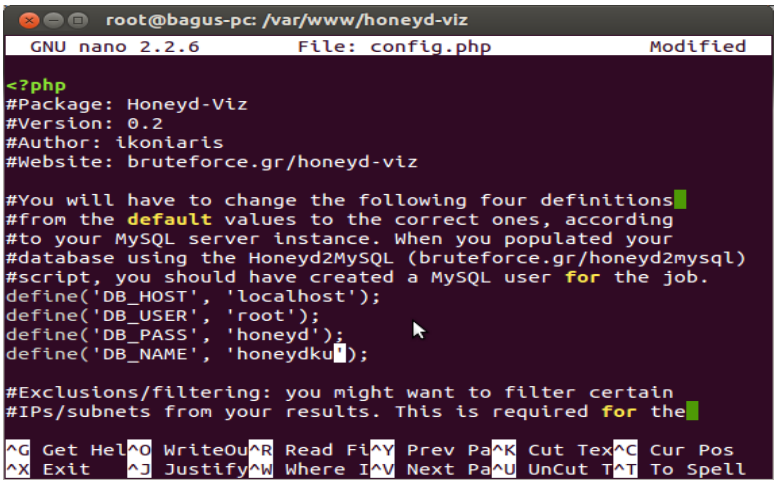
Gambar 4. Konfigurasi honeydku.conf

Berikut keterangan dari konfigurasi Honeyd Berdasarkan Gambar 4 :

1. Create default = memberikan konfigurasi agar tcp, udp dan icmp agar ter block secara default.
2. Create linux = memberikan konfigurasi nama linux, nama bisa kita rubah sesuai dengan keinginan.
3. Set linux personality “Linux 2.0.35 (S.u.S.E. Linux 5.3 i386)” = konfigurasi personality digunakan untuk mengadaptasi sistem informasi linux suse dan mengelabui scanner fingerprint seperti nmap, network scanner, ipscan dll.
4. Set linux default tcp action block = memberikan konfigurasi pada honeyd untuk memblock setiap koneksi ke tcp secara default.
5. Add linux tcp port 21 open = memberikan konfigurasi pada honeyd untuk membuka koneksi ke tcp port 21 agar terbuka.
6. Add linux tcp port 22 open = memberikan konfigurasi pada honeyd untuk membuka koneksi ke tcp port 22 agar terbuka.
7. Add linux tcp port 23 open = memberikan konfigurasi pada honeyd untuk membuka koneksi ke tcp port 23 agar terbuka.
8. Add linux tcp port 80 open = memberikan konfigurasi pada honeyd untuk membuka koneksi ke tcp port 80 agar terbuka.
9. Set linux Ethernet “Dell” = memberikan konfigurasi pada honeyd untuk memberikan nama vendor Ethernet yang akan digunakan.
10. Bind 172.19.11.101 linux = memberikan konfigurasi pada honeyd untuk memberikan IP address kepada honeyd.

Sebelum melakukan instalasi Honeyd-viz ada beberapa packages library dan aplikasi yang harus di install terlebih dahulu agar honeyd bisa berjalan dengan baik, seperti honeyd2mysql , Mysql, Apache, Php5. Aplikasi honeyd-viz digunakan untuk menampilkan

hasil log secara visual agar mempermudah administrator untuk menganalisa hasil serangan pada honeyd.



Gambar 5. Konfigurasi honeyd-Viz

Berdasarkan gambar 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.

4.1. Scanning Host dan Port

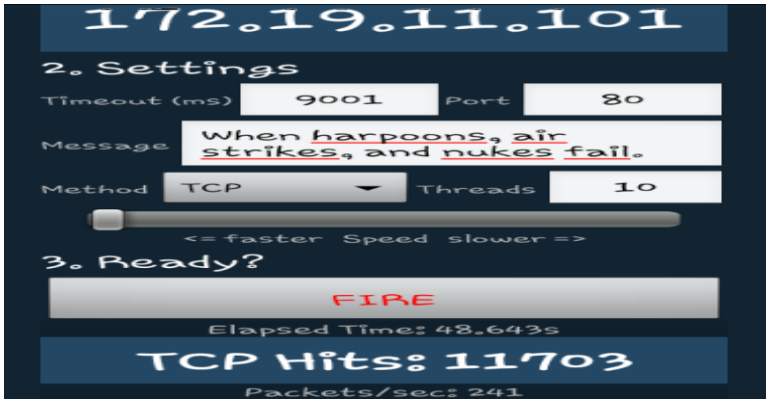
Pengujian serangan yang akan dilakukan adalah host scanning dan port scanning yang bertujuan untuk mengetahui host yang sedang aktif. Berikut adalah proses scanning host dan port pada jaringan yang dilakukan oleh attacker menggunakan Net Scan.

Gambar 6. Proses Scanning Host dan Port

Pada gambar 6 terlihat bahwa scanning yang dilakukan Netscan dapat mendeteksi dengan baik host yang diciptakan oleh honeyd, pada proses scanning terlihat bahwa beberapa port host honeyd dengan ip 172.19.11.101 dapat terdeteksi dengan baik oleh Netscan yaitu port 21 untuk ftp, port 22 untuk ssh, port 23 untuk telnet dan port 80 untuk http.

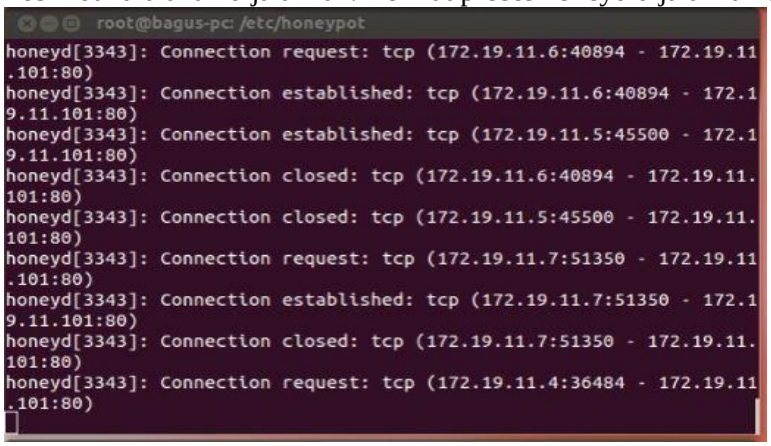
4.2. Serangan Tcp Flood

Berikut adalah proses serangan TCP flood pada host honeyd yang dilakukan oleh attacker menggunakan Loic.



Gambar 7. Proses Serangan Tcp Flood dengan Loic

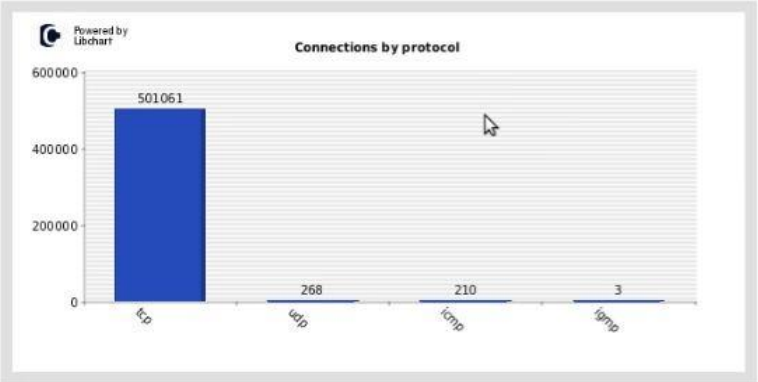
Berdasarkan Gambar 7 terdapat ip honeyd yang akan diserang yaitu ip 172.19.11.101, port 80, method yang digunakan adalah TCP, threads yang diisikan 10, serta pengaturan kecepatan penyerangan dengan merubah slider kearah faster. Sebelum melakukan serangan maka honeyd terlebih dahulu akan dijalankan. Berikut proses honeyd dijalankan :



Gambar 8. Proses Honeyd Mendeteksi Serangan Tcp Flood

Berdasarkan Gambar 8 merupakan proses honeyd dalam mendeteksi serangan yang terjadi. Terlihat beberapa ip yang melakukan akses terhadap honeyd yang mempunyai ip 172.19.11.101 dan port yang dituju adalah port 80 dengan method yang digunakan adalah TCP.

Berikut tampilan data log honeyd yang telah diload ke honeyd-viz.

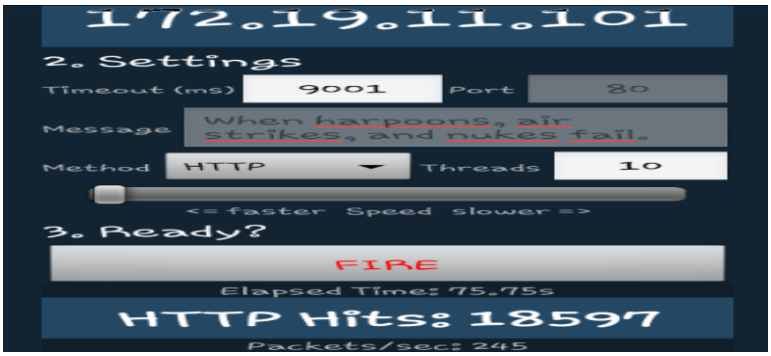


Gambar 9. Tcp flood Honeyd-viz Connections By Protocol

Dari gambar 9 terlihat bahwa koneksi dengan protocol tcp sebesar 501061, udp sebesar 268, icmp sebesar 210 dan igmp sebesar 3.

4.3. Serangan Http Flood

Berikut adalah proses serangan Http flood pada host honeyd yang dilakukan oleh attacker menggunakan Loic.



Gambar 10. Proses Serangan Http Flood dengan Loic

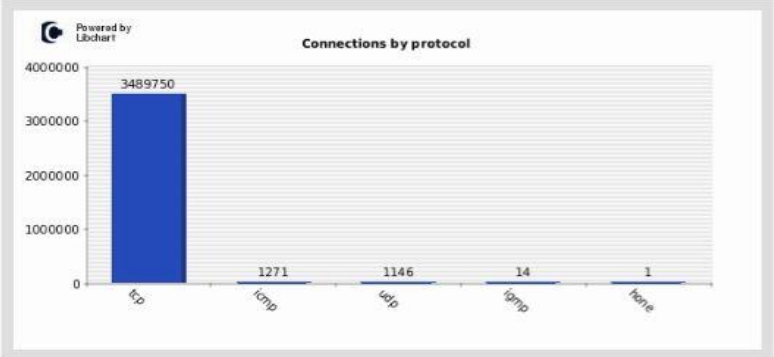
Berdasarkan Gambar 10 terdapat ip honeyd yang akan diserang yaitu ip 172.19.11.101, port 80, method yang digunakan adalah Http, threads yang diisikan 10, serta pengaturan kecepatan penyerangan dengan merubah slider kearah faster. Sebelum melakukan serangan maka honeyd terlebih dahulu akan dijalankan. Berikut proses honeyd dijalankan :

```
honeyd[3716]: Connection closed: tcp (172.19.11.6:46024 - 172.19.11.
101:80)
honeyd[3716]: Connection closed: tcp (172.19.11.5:60679 - 172.19.11.
101:80)
honeyd[3716]: Connection closed: tcp (172.19.11.5:41971 - 172.19.11.
101:80)
honeyd[3716]: Connection established: tcp (172.19.11.6:56407 - 172.1
9.11.101:80)
honeyd[3716]: Connection closed: tcp (172.19.11.6:34552 - 172.19.11.
101:80)
honeyd[3716]: Connection established: tcp (172.19.11.6:50414 - 172.1
9.11.101:80)
honeyd[3716]: Co
```

Gambar 11. Proses Honeyd Mendeteksi Serangan Http Flood

Berdasarkan Gambar 11 merupakan proses honeyd dalam mendeteksi serangan yang terjadi. Terlihat beberapa ip yang melakukan akses terhadap honeyd yang mempunyai ip 172.19.11.101 dan port yang dituju adalah port 80 dengan method yang digunakan adalah TCP.

Berikut tampilan data log honeyd yang telah diload ke honeyd-viz.



Gambar 12. Http flood Honeyd-viz Connections By Protocol

Berdasarkan gambar 12 terlihat bahwa koneksi dengan protocol tcp sebesar 3489750, icmp sebesar 1271, udp sebesar 1146, igmp sebesar 14.

4.4. Serangan Udp Flood

Berikut adalah proses serangan Udp flood pada host honeyd yang dilakukan oleh attacker menggunakan Loic.

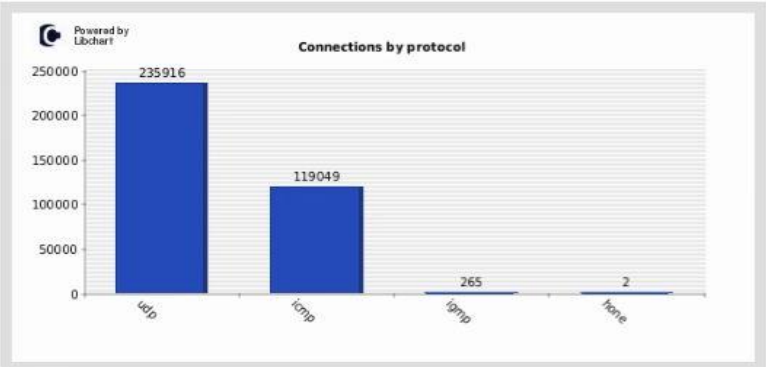
Gambar 13. Proses Serangan Udp Flood dengan Loic

Berdasarkan Gambar 13 terdapat ip honeyd yang akan diserang yaitu ip 172.19.11.101, port 80, method yang digunakan adalah Udp, threads yang diisikan 10, serta pengaturan kecepatan penyerangan dengan merubah slider kearah faster. Sebelum melakukan serangan maka honeyd terlebih dahulu akan dijalankan. Berikut proses honeyd dijalankan :

```
honeyd[3426]: Connection to closed port: udp (172.19.11.4:36184 -
172.19.11.101:80)
honeyd[3426]: Connection to closed port: udp (172.19.11.4:45718 -
172.19.11.101:80)
honeyd[3426]: Connection to closed port: udp (172.19.11.5:49230 -
172.19.11.101:80)
honeyd[3426]: Connection to closed port: udp (172.19.11.5:45163 -
172.19.11.101:80)
honeyd[3426]: Connection to closed port: udp (172.19.11.5:52067 -
172.19.11.101:80)
honeyd[3426]: Connection to closed port: udp (172.19.11.4:47244 -
172.19.11.101:80)
```

Gambar 13. Proses Honeyd Mendeteksi Serangan Http Flood

Berdasarkan Gambar 13 merupakan proses honeyd dalam mendeteksi serangan yang terjadi. Terlihat beberapa ip yang melakukan akses terhadap honeyd yang mempunyai ip 172.19.11.101 dan port yang dituju adalah port 80 dengan method yang digunakan adalah Udp. Berikut tampilan data log honeyd yang telah diload ke honeyd-viz.

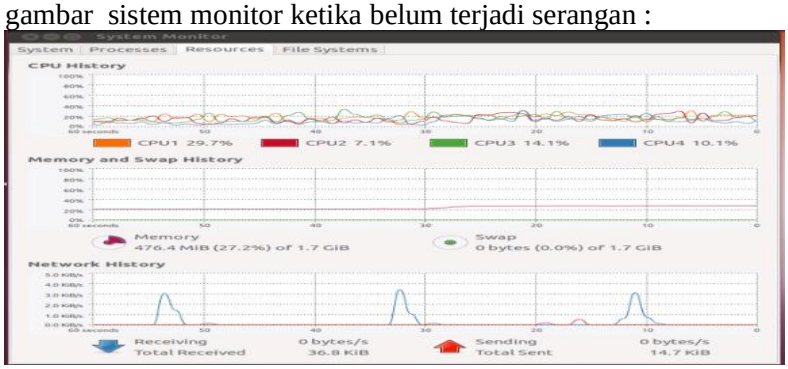


Gambar 14. Udp flood Honeyd-viz Connections By Protocol

Berdasarkan gambar 14 terlihat bahwa koneksi dengan protocol Udp sebesar 235916, icmp sebesar 119049 dan igmp sebesar 265, none 2.

4.5. Serangan Ddos ke Server

Pengujian selanjutnya yang dilakukan adalah serangan TCP Flood terhadap server. Berikut adalah gambar sistem monitor ketika belum terjadi serangan :



Gambar 15. Sistem Monitor Sebelum Serangan ke Server

Pada gambar 15 sebelum terjadinya serangan terlihat bahwa CPU History menunjukkan beban kerja CPU1 sebesar 29,7%, CPU2 sebesar 7,1%, CPU3 sebesar 14,1%, CPU4 sebesar 10,1% dan memory 27.2%.

Gambar 16. Sistem Monitor Serangan ke Server

Pada gambar 16 ketika terjadinya serangan terlihat bahwa CPU History menunjukkan peningkatan beban kerja CPU1 sebesar 48,9%, CPU2 sebesar 48,0%, CPU3 sebesar 46.%, CPU4 sebesar 40,9%, dan memory 28.9%.

.

Gambar 17. Sistem Monitor Setelah Pembelokkan Serangan

Pada gambar 17 ketika terjadinya serangan yang diblok oleh iptables terlihat bahwa CPU History menunjukkan penurunan beban kerja CPU1 sebesar 31,3%, CPU2 sebesar 31,4%, CPU3 sebesar 31,1%, CPU4 sebesar 29,5%, dan memory 28.2%. Agar memudahkan dalam membaca analisa maka akan dibuat tabel perbandingan sebelum penyerangan, setelah penyerangan dan setelah penyerangan dibelokkan.

Tabel 1 Perbandingan Serangan TCP Flood ke Server

No	Cpu History	Sebelum Serangan	Setelah Serangan	Setelah Pembelokkan
1	Cpu1	29.7%	48.9%	31.3%
2	Cpu2	7.1%	48.0%	31.4%
3	Cpu3	14.1%	46.1%	31.1%
4	Cpu4	10.1%	40.9%	29.5%
5	Memory	27.2%	28.9%	28.2%

Dari tabel 1 terlihat bahwa ada kenaikan beban kerja cpu1, cpu2, cpu3, cpu4 dan memory pada server, setelah adanya pembelokkan dengan iptables beban kerja cpu1, cpu2, cpu3, cpu4 dan memory server terjadi penurunan.

5. Kesimpulan

Dari hasil pengujian, penulis dapat menyimpulkan bahwa :

1. Honeyd dapat memberikan servis yang mirip seperti komputer asli kepada attacker dan juga dapat mendeteksi serangan Ddos secara real time .
2. Dengan Penggunaan Iptables sebagai firewall serangan ddos dapat dibelokkan ke ip yang tidak digunakan. Beban rata-rata kinerja cpu sebelum terjadi serangan sebesar 15.25% Setelah adanya serangan beban rata-rata kinerja cpu naik menjadi 45.98% setelah adanya pembelokkan serangan dengan iptables beban rata-rata kinerja cpu menurun menjadi 30.83%.

Daftar Pustaka

Sivaprakasam, V, dan Nirmal sam,S. (2014) .Achieving Higher Network Security By Preventing DDOS Attack Using Honeypot. ISSN (Online) 2 (2). 2347-2812.

Firrar, Utdirartatmo. (2005). Trik Menjebak Hacker Dengan Honeypot. Yogyakarta: Penerbit Andi.

Farunuddin, Rakhmat. (2005). Membangun Firewall dengan IPTables di Linux. Jakarta: PT. Elex Media Komputindo.

Purbo, W Onno, Adnan Basalamah, Ismail Fahmi, dan Achmad Husni Thamrin, (1998). TCP/IP. Jakarta: PT. Elex Media Komputindo.

Setyo, A.N., Raharjo, S. dan Triyono, J (2013). Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan. Jurnal Jarkom 1 (1). 40-48.

Mustofa, M.M. dan Aribowo, E. (2013) . Penerapan Sistem Keamanan Honeypot Dan IDS Pada Jaringan Nirkabel (Hotspot). Jurnal Sarjana Teknik Informatika 1(1). 111-118.

Ariyus, Dony, M.Kom. (2007). Intrusion Detection Sytem : Sistem Pendeteksi Penyusupan Pada Jaringan Komputer. Yogyakarta: Penerbit Andi

Anjik, Sukamaaji, S.Kom. Rianto, S.Kom. (2008). Konsep Dasar Pengembangan Jaringan Dan Keamanan Jaringan. Yogyakarta: Penerbit Andi.