PENDETEKSI SERANGAN DDoS (*DISTRIBUTED DENIAL OF SERVICE*) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI

Saleh Dwiyatno[1], Ayu Purnama Sari[2], Agus Irawan[3], Safig[4]
Universitas Serang Raya
Jl. Raya Serang Cilegon Drangong Taktakan Kota Serang Banten
Email : salehdwiyatno@gmail.com[1], Ayupurnamasarifaliza@gmail.com[2], irawanagus.2015@gmail.com3, safig@gmail.com[4]

ABSTRACT

Information security is very important in today's technology. Information storage and crossing is currently no longer using paper media, but has used a lot of computer and internet media. PT. Torini Jaya Abadi is one that uses computer and internet media for information storage and crossing. However, there are disturbances such as heavy server access, which cannot be accessed and sometimes it cannot enter into the database server from the indication that the server might be exposed to a virus or DDoS (Distributed Danial of Service) type attacks occur on the server. Based on these problems, the author uses a honeypot to detect an attack based on alerts that have been accommodated in the log and can also provide information about the attacks that occur, from the results obtained honeyd is able to resemble an original system that pretends to have services that are not real , also able to detect attacks in real time and provide information from attackker, honeyd can emulate virtual hosts that are similar to the original computer, by obtaining logs from the honeyd admin system to find out information that occurs on the server, with honeyd network systems can help detect attacks in real time.

***Keywords** : DDoS, Honeypot, Honeyd, Network, Server*

PENDAHULUAN

Keamanan informasi sangat penting diera teknologi sekarang ini. Penyimpanan informasi saat ini tidak lagi menggunakan media kertas, tetapi sudah banyak menggunakan teknologi komputer dan *internet*. Karena jaringan merupakan ruang *public*, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut. Disisi lain, terdapat pihak-pihak dengan maksud tertentu yang berusaha untuk menembus sistem keamanan, begitu pula dengan adanya tindakaan penyusup, ancaman keamananpun sangat beragam, mulai dari *virus* atau *worm*, *malware*, penanaman *backdoor*, hingga penyerangan *distributed danial of service* yang menyebabkan *server* akan mati dan tidak dapat beroprasi lagi sehingga otomatis tidak dapat memberikan pelayanan. Berbagai ancaman keamanan teknologi informasi dapat diminimalkan dengan memaksimalkan identifikasi celah keamanan sedini mungkin (Aidin, Nasution, dan azmi 2016)

Mengelola potensi bisnis khususnya dalam bidang pekerjaan instrumen listrik, PT. Torini Jaya Abadi membangun jaringan *internet* yang dipergunakan untuk mengakses *server*, yang terdiri dari *database server, web aplication server*, dan untuk mengakses aplikasi tersebut PT. Torini Jaya Abadi membuat akses yaitu melalui akses yang terkoneksi dengan *internet*. Menurut hasil wawancara dengan bapak Budi Cahyono sebagai staff, pada PT. Torini Jaya Abadi sering kali terjadi gangguan seperti, akses pada *server* yang sangat berat, yang tidak dapat diakses dan terkadang tidak dapt masuk ke dalam *database server*, disebabkan komputer yang terkoneksi pada infrastruktur jaringan dan memiliki akses ke *server* tidak terjamin bebas *virus, spyware, malwarae,* dan semacamnya.

Dari indikasi-indikasi tersebut terdapat kemungkinan jika *server* tersebut terkena *virus* dari komputer-kompuuter yang terkoneksi pada *server* atau terjadi serangan pada *server*, baik seperti *trojan*, DoS *attack* ataupun DDoS, *malware* atau yang biasa di sebut perangkat perusak. Apabila terjadi gangguan pada *server* maka penginputan data akan terganggu dan akan berakibat keterlambatan dikarnakan laporan pada aplikasi dikunci dengan tanggal penginputan dan sangat berbahaya apabila data yang terdapat pada *server* menjadi rusak atau *corrupt*.

Sistem keamanan *firewall* tidak cukup meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator tidak bisa mengetahui dengan pasti apa yang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk mengaudit sistem guna mencari permasalahan yang telah terjadi. Serangan yang paling sering digunakan adalah DDoS (*Distributed Denial of service*). sistem *honeypot* merupakan sistem keamanan komprehensif meskipun *honeypot* memiliki ruang lingkup deteksi dan respon. Namun dapat merekam semua kemungkinan celah kemanan.

Berdasarkan dari masalah tersebut, maka penulis menggunakan *honeypot* agar dapat mendeteksi suatu serangan berdasarkan *alert* yang telah ditampung pada *log* dan juga dapat memberikan informasi tentang serangan yang terjadi.

Berdasarkan latar belakang masalah yang telah dipaparkan, masalah dapat diindentifikasikan sebagai berikut :

1. Ancaman serangan dalam bentuk DDoS (*Distributed Denial of Service*).
2. Kurangnya keamanan yang responsif terhadap ancaman serangan.

3. Tidak adanya monitoring keamanan pada *server.*

Berdasarkan uraian di atas mengenai pendeteksian serangan DDoS (*Distributed Denial of Service*), maka peneliti merumuskan masalah sebagai berikut:

1. Bagaimana pendeteksi *honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan?
2. Jenis Honeypot yang akan digunakan adalah Honeyd?
3. Bagaimana memonitor keamanan jaringan yang responsif dengan *honeypot?*

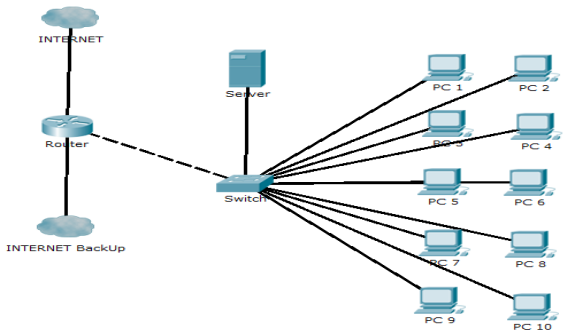
PEMECAHAN MASALAH

Manajemen Jaringan

Manajemen jaringan merupakan kemampuan untuk mengontrol dan memonitor suatu jaringan komputer yang meliputi diantaranya topologi jaringan, arsitektur jaringan, skema jaringan, keamanan jaingan dan spesifikasi *hardware* dan *software* jaringan.

Topologi Jaringan

Topologi yang digunakan di PT. Torini Jaya Abadi adalah topologi mesh. Topologi mesh yaitu suatu hubungan antar prangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada pada jaringan. Jadi dalam topologi mesh setiap perangkat dapat saling berkomunikasi langsung dengan perangkat yang dituju.



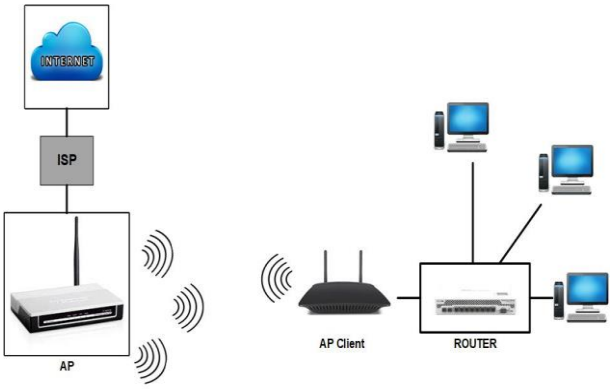
Gambar 1 Topologi Jaringan PT. Torini Jaya Abadi

PT Torini Jaya Abadi memiliki satu *extranet* sebagai *backlink* yang berguna sebagai cadangan koneksi internet. *ExtraNet* menggunakan jaringan *protocol* TCP/IP untuk menghubungkan berbagai *internet* pada lokasi berbeda. *Extranet* bermanfaat dalam mewujudkan konektivitas yang aman antara *internet* perusahaan

dan *internet* mitra bisnis, penyedia massa, *financial*, pemerintan dan pelanggan. Lingkungan eksternal yang terproteksi memungkinkan setiap kelompok untuk berkolaborasi, berbagi informasi secara ekslusif dan bertukar informasi secara aman

Arsitektur Jaringan

Secara umum sistem jaringan *internet* mempunyai dua konfigurasi, yaitu dengan mode Ad-Hoc dan mode arsitektur, tetapi di PT. Torini Jaya Abadi lebih menggunakan mode arsitektur karena efesiensi dan hemat biaya. mode arsitektur Jaringan *internet* yang bekerja pada mode Ad-Hoc hanya dibatasi untuk hubungan antar ketiga komputer. Untuk menghubungkan banyak komputer, jaringan harus dijalankan menggunakan mode arsitektur. Untuk menyusun jaringan yang bekerja pada mode arsitektur diperlukan peralatan tambahan berupa *wireless access* point (WAP) atau disebut secara singkat dengan *access point* (AP) mempunyai fungsi seperti *hub* atau *switch* pada jaringan kabel, maka *access point* akan menjadi *cente*r dari jaringan *internet*. Bentuk jaringan *internet* dengan *access point* di PT. Torini Jaya Abadi dapat disimulasikan pada gambar berikut.



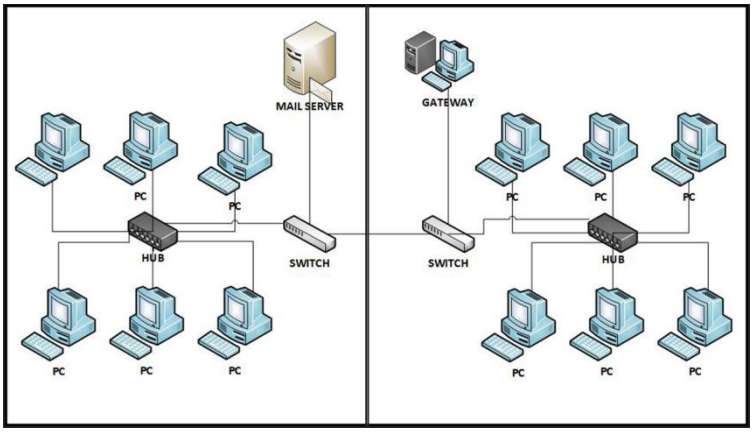
Gambar 2 Simulasi Mode Arsitektur PT. Torini Jaya Abadi

Pada jaringan di PT. Torini Jaya Abadi masing-masing komputer akan saling berhubungan melalui AP (*Access Point*). Jumlah komputer yang bisa terhubung ke jaringan sangat tergantung pada kemampuan *access point* dalam melayani *clien*. Sama seperti kemampuan *switch* dalam menyediakan jumlah *port*. Luas daerah yang dapat dijangkau oleh *access point* tergantung pada peralatan yang dipakai. Untuk mencapai jangkauan lebih luas, jaringan *internet* di PT. Torini Jaya Abadi sudah dilengkapi dengan *extention point*. *Extention point* berfungsi menguatkan isyarat yang dipancarkan *access point* dan memancarkan kembali isyarat tersebut. *Extention point* mempunyai fungsi yang sama seperti *repeater* pada jaringan

kabel,di PT. Torini Jaya Abadi diinstalasi menggunakan mode infrastruktur ini karena sangat cocok dengan kondisi gedung dan terdiri dari beberapa gedung.

Skema Jaringan

PT. Torini Jaya Abadi mempunyai ISP (*Internet Service Provider*) yang terhubung ke *Router* utama, *Wireless Backup link* serta *Access point*. PT. Torini Jaya Abadi juga memiliki satu *Extranet* sebagai *Backup internet Access point* tersebut terhubung ke setiap *router*. *Router* utama juga terhubung ke DNS *server*, *server email* dan *server farm* . Gambar 3.4 ini adalah topologi jaringan per-gedung PT. Torini Jaya Abadi:



Gambar 3 Skema Jaringan PT. Torini Jaya Abadi

Berdasarkan gambar 3 adalah skema jaringan PT. Torini Jaya Abadi terdapat dua bangunan terpisah (*building block*) yang terdiri dari Gedung A, Gedung B. Masing-masing gedung pada umumnya telah memiliki personal komputer dan telah diintegrasikan dengan suatu jaringan *intranet* yang dipusatkan pada *Mail Server Litbang* di Gedung A lantai 1, menggunakan topologi star karena telah memakai *active Hub*, jalur *back bone* untuk mengcascade antar *hub* maupun dari *hub* ke *Client* semuanya. menggunakan kabel UTP. *Workstation Intranet* terbanyak berkumpul gedung utrama.

Terpisahnya gedung di area PT. Torini Jaya Abadi dengan jarak dan tingkat kesulitan yang variatif akan memaksa mengkondisikan sistem teknologi yang di atas standard normal dengan menuntut teknologi canggih yang menjamin *performance*, *securitas*, *speed* yang memadai sesuai dengan tuntutan *user*.

PT. Torini Jaya Abadi memanfaatkan kabel *Fiber Optic* untuk dijadikan infrastruktur jaringan. Selain kecepatan transfer data yang dapat diandalkan FO

juga tahan terhadap kilatan petir. Jaringan *active hub* ke *client* tetap menggunakan UTP.

Keamanan Jaringan

Untuk pengamanan jaringn PT. Torini Jaya Abadi Menggunakan *Wireleess Protector Enterprice* 1.3 manajemen *software* ini berbasis *windows* dan perangkat lunak keamanan yang secara otomatis menonaktifkan *WiFi adapter* pada komputer yang terhubung ke jaringan LAN PT. Torini Jaya Abadi dan kembali mengaktifkan *WiFi* ketika kabel LAN diputus dari komputer *nirkabel*. *Software* ini bertindak sebagai *server* untuk semua komputer *nirkabel* dilindungi dan perlu diinstal hanya sekali pada *platform windows* aktif yang dihubungkan dengan kabel LAN.

Spesifikasi Sofware dan Hardware Jaringan

1. *Software*

   Alat-alat yang di gunakan untuk mendukung *software* di PT. Torini Jaya Abadi cuckup bervariasi di antaranya sebagai berikut.

   a. *Ubuntu*
   b. *Apache*
   c. Windows
   d. *Mysql*
   e. Nmap
   f. *Wireleess Protector Enterprice 1.3*
   g. Winbox

2. *Hardware*

   Alat-alat yang digunakan untuk mendukung *Hardware* di PT. Torini Jaya Abadi suduh memenuhi syarat standar di antaranya sebagai berikut.

   a. *Modem*
   b. *Hub*
   c. *Switch*
   d. *Kabel UTP*
   e. *Access point*
   f. *USB Wireless*

Permasalahan Sistem Jaringan

Hasil yang didapatkan setelah melakukan kunjungan dan pengamatan di PT. Torini Jaya Abadi bahwa sering kali terjadinya gangguan seperti akses *server* yang sangat berat, yang tidak bisa diakses dan terkadang tidak dapat masuk kedalam *database server*. Dari indikasi tersebut kemungkinan *server* terkena *virus,* atau terjadi serangan jenis DDoS (*Distributed Denial of Service*) pada *server.*

Alternatif Pemecahan Masalah

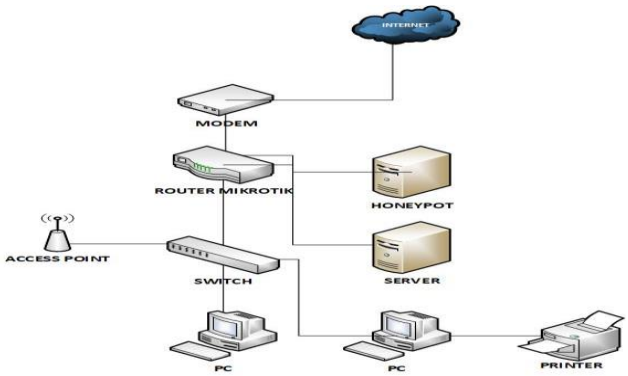
Peningkatan Dari ancaman serangan jaringan pada PT. Torini Jaya Abadi memerlukan suatu sistem pendeteksi untuk jaringan komputer. Perlindungan *server*

dan *database server* yang digunakan dari analisis pada PT. Torini Jaya Abadi akan diusulkan memakai sistem aplikasi *honeypot* sebagai pendeteksi serangan jaringan DDoS (*Distributed Danial of Service*).

IMPLEMENTASI

Topologi Jaringan

Pada rancanga jaringan usulan, tetap mengunakan topologi mesh di karenakan fleksibel, pengelolaan dan pengembangan jaringa lebih mudah, perawatan yang dilakukan di suatu *node* maupun kerusakan pada suatu *node* tidak mempengaruhi *node* yang lainnya, kemudahan dalam pengelolaan jaringan, deteksi dan kesalahan lebih mudah, hanya saja menambahkan *honeypot* sebagai pendeteksi serangan DDoS (*Distributed Denial of Servic*).



Gambar 4 Topologi Jaringan Usulan

Sekema Jaringan

Berdasarkan dari analisa permasalahan yang dihadapi maka penulis melakukan penambahan dalam sekema jaringan yang sudah ada, penulis hanya menambakan *software* atau *aplikasi* yang difungsikan sebagai sistem pendeteksi dengan tujuan utama penyerangan yang sebenarnya merupakan sistem yang palsu untuk menjebak penyerang dan pendeteksi biasanya di hubungkan dengan jaringan produktif atau yang asli pada PT. Torini Jaya Abadi.

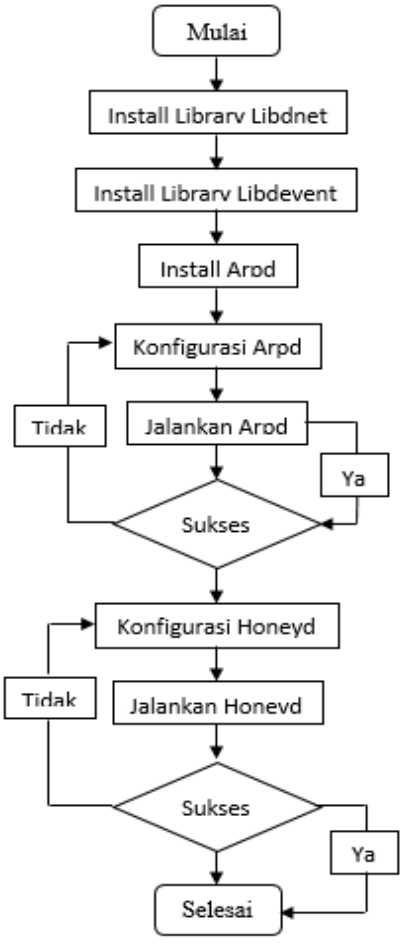
Keamanan Jaringan

Komponen yang paling penting dalam membangun sebuah jaringan komputer yaitu mengenai *firewall* berserta celah-celah keamanan jaringan sendiri, dalam suatu jaringan internal perusahaan membutuhkan keamanan khusus yang dapat menjaga data-data penting dari serangan pihak-pihak dengan maksud tertentu yang berusaha untuk menembus sisten keamanan.

Untuk kemanan jaringan pada PT. Torini Jaya Abadi sistem keamanan jaringan yang diterapkan menggunakan *Wireleess Protector Enterprice 1.3*, hanya saja aplikasi ini untuk keamanan sistem tertentu. Untuk itu penulis menambahkan rancangan unsulan keamanan menggunakan aplikasi *honeypot*. Aplikasi ini mampu untuk mendeteksi dan memanipulasi serangan yang ada, untuk menjebak penyerang.

Rancangan Aplikasi

Pada rancangan aplikasi ini penulis mengusulkan *software* yang di gunakan untuk monitoring dan mendeteksi penyerangan pada perangkat *server* di jaringan komputer PT. Torini Jaya Abadi menggunakan *software honeypot*, Adapun cara menerapkan *software honeypot* sebagai berikut:

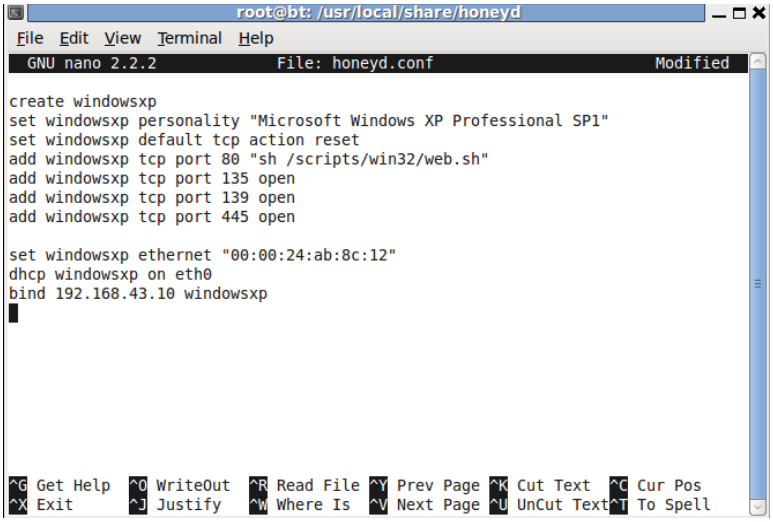


Gambar 5 Alur Rancangan Honeypot

Pada alur rancangan *honeypot* secara sederhana menjelaskan bahwa sebelum menjalankan *honeyd* terlebih dahulu menginstal *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 atau tidak sukses maka akan kembali lagi ke proses konfigurasi arpd, dan jika sukses maka ke proses selanjutnya yaitu konfigurasi *honeyd* dan menjalankan *honeyd*. Jika menjalankan *honeyd* menemukan kendala atau tidak sukses maka akan kembali lagi ke proses konfigurasi *honeyd* dan jika sukses maka *honeyd* dapat digunakan.

Setelah instal berhasil, selanjutnya buat file konfigurasi untuk *honeyd* dengan mengetikan perintah nano honeyd.conf pada terminal maka akan dibawa ke *directori honeyd*.



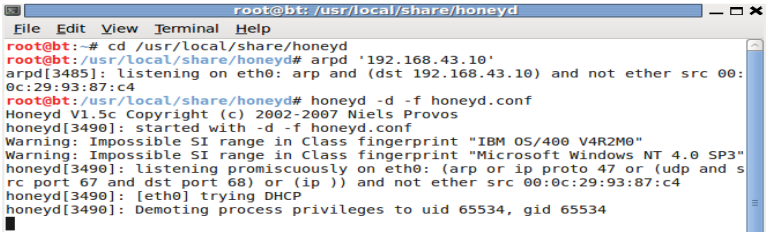
Gambar 6 Konfigurasi Honeyd.Conf

Berdasarkan gambar 6 dalam pengertian konfigurasi honeyd.conf sebagai berikut :

1. *Create windowsxp* : memberi nama pada konfigurasi, nama tersebut bisa diisi dengan sesuai keinginan, nama tersebut juga berfungsi sebagai variabel yang dapat di panggil.
2. *Set windowsxp personality* "*Mictodoft Windows XP Professional* SP1" : personality digunakan untuk sistem operasi tertentu untuk mengelabuhi *scanner fingerpint* semacam Nmap dan ketika *device* lain terkoneksi dengan *honeyd* ini maka akan di kenali sebagai *Windows* XP SP1.
3. *Set windowsxp default tcp action reset* : menyatakan akan menghentikan traffic yang tidak termasuk open *port* yang didefinisikan pada file konfigurasi.
4. *Add windowsxp tcp port* 80 "sh *honeyd/scripts/web*.sh" : menyatakan bahwa port 80 pada tcp dibuka.
5. *Add windowsxp tcp port* 135 : menyatakan bahwa port 135 pada tcp di buka.

6. *Add windowsxp tcp port* 139 : menyatakan bahwa port 139 pada tcp di buka.
7. *Add windowsxp tcp port* 445 : menyatakan bahwa port 445 pada tcp di buka.
8. *Set windowsxp ethernet* "00:00:24:ab:8c:12" dan dhcp *windowsxp on* eth0 : menyatakan mengeset MAC *address*, hal ini di butuhkan jika menjalankan *honeyd* dengan dhcp
9. *Bind* 192.168.43.10 *windowsxp* : menyatakan bahwa *Ip address* 192.168.43.10 digunakan oleh baris konfigurasi *windowsxp* dan IP tersebut digunakan sebagai ip *honeyd*.

Setelah konfigurasi selesai di masukan, selanjutnya lakukan tes apakah arpd dan *honeyd* sudah dapat berjalan atau belum, dengan memasukan perintah sebagai berikut :



Gambar 7 Tampilan Honeyd dan arpd Saat Dijalankan

Berdasarkan gambar 7 tampilan arpd dan *honeyd* saat di jalankan, penjelasannya adalah sebagai berikut :

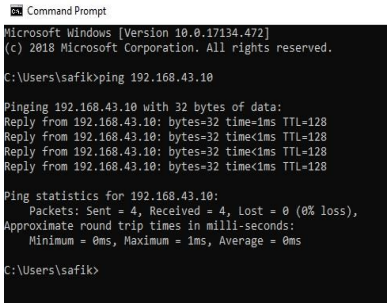
Arpd 192.168.43.10 adalah *Ip address honeyd* yang harus dilakukan karna aplikasi arpd merupakan *daemon* yang mendengarkan perintah ARP dan jawaban untuk alamat IP yang tidak terpakai atau terisi.

Untuk menjalankan honeyd adalah dengan mengetikan pertintah honeyd -d -f honeyd.conf.

-d : digunakan untuk menampilkan *alert* secara *real time*, jika tidak menggunakan -d maka *honeyd* akan berjalan secara *background*.

-f : digunakan untuk mengambil file konfigurasi honeyd.conf jika tidak menggunakan -f maka *honeyd* akan berjalan dengan konfigurasi *default*.

untuk membuktikan bahwa tes koneksi *ping* terhadap *honeyd* apakah sudah terkoneksi atau belum, dimana *IP honeyd* terdapat pada *subnet class IP* tersebut seperti pada gambar 4.5

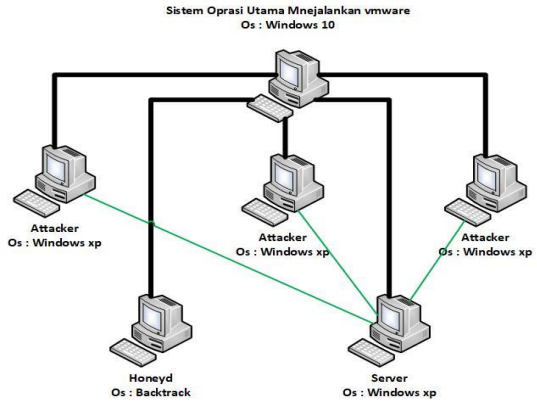


Gambar 8 Koneksi honeyd

Setelah terkoneksi bisa dilihat informasi *ping* dengan *IP honeyd* 192.168.43.10 informasi TTL di atas biasanya juga dipakai *attacker* untuk menentukan apakah sedang berhadapan dengan *host* asli atau *honeypot.*

Pengujian Jaringan

Dalam hal membangun jaringan komputer perlu dilakukan sebuah pengujian terhadap jaringan yang telah dibangun, maka penulis membuat pengujian jaringan serangan secara sederhana seperti terlihat gambar 9

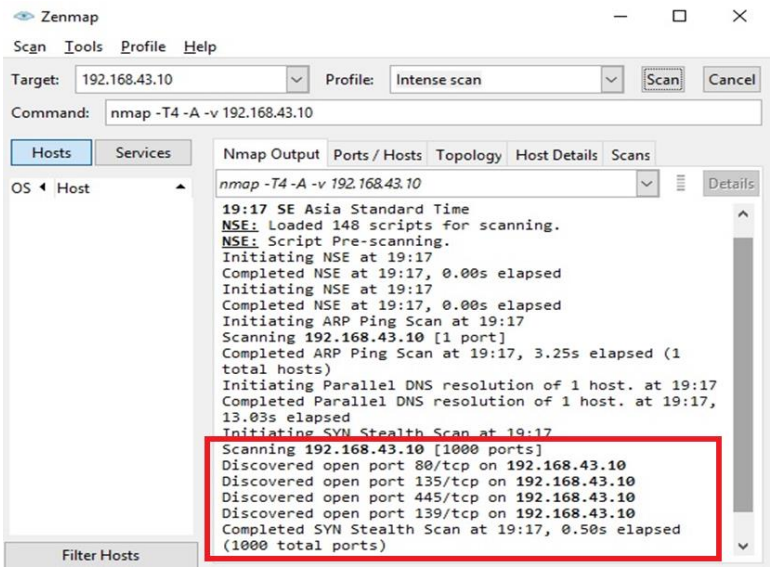


Gambar 9 Simulasi Jaringan Serangan

Seperti yang tertera pada gambar 9 secara sederhana menjelaskan bahwa sistem oprasi utama menjalankan aplikasi *vmware* yang mana nantinya akan menjalankan beberapa OS untuk simulasi serangan, ketiga OS *windows* xp akan menjadi *attacker* kemudian diperintah untuk menyerang *server* dan nantinya *honeyd* nantinya akan mendeteksi serangan yang berada pada sistem oprasi *backtrack.*

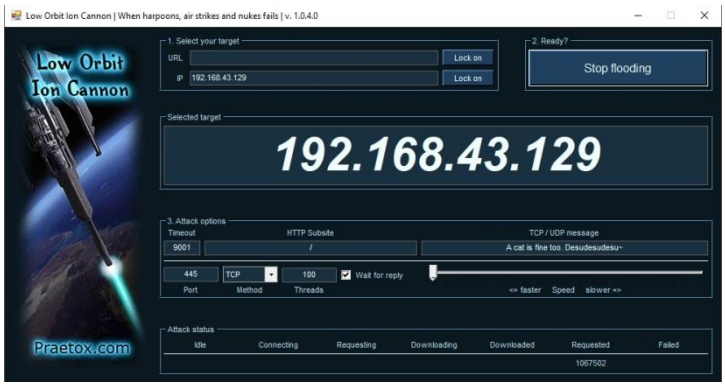
Pengujian Jaringan Awal

Pada pengujian jaringan awal ini pertujuan untuk membuktikan bahwa *scanning* yang di tunjukan oleh *zenmap*, dimana terdapat pada *subnet class IP* tersebut seperti pada gambar 10



Gambar 10 Hasil *Port Scanning*

Berdasarkan gambar 10 setelah melakukan *scanning* pada *honeyd* menggunakan *zenmap* dapat medeteksi dengan baik *host* yang diciptakan oleh *honeyd*, pada proses *scanning* terlihat bahwa beberapa *port host honeyd* dengan IP 192.168.43.10 dapat terdeteksi dengan baik oleh *zenmap* yaitu *port-port* yang terbuka, yang berpura-pura memiliki *service-service* yang tidak nyata untuk menarik perhatiaan para *attacker* atau mengalihkan perhatian mereka dari sistem yang sebenarnya, dan serangan DDoS akan di uji coba secara langsung dengan menyerang *server* bisa dilihat pada gambar 11

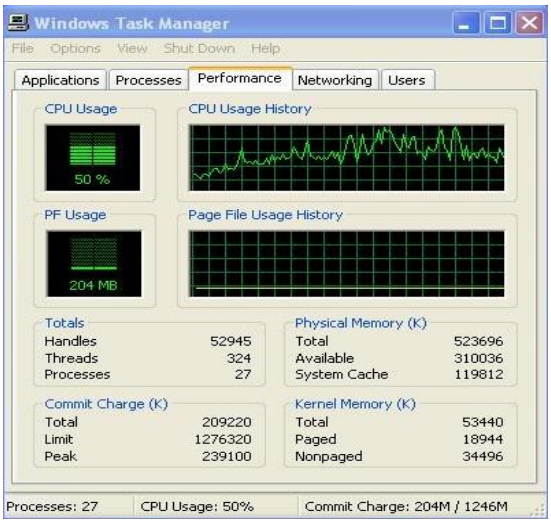


Gambar 11 Serangan DDoS Terhadapt Server

Pada *tools* LOIC akan menyerang menggunakan perintah IP 192.168.43.129 *port* 445, *melhod* TCP, threads 100 serta pengaturan kecepatan penyerang dengan merubah *slider* kearah *faster*. Setelah menjalankan serangan DDoS (*Distributed Denial of Service*) maka selanjutnya pada PC akan terlihat dampak yang dihasilkan oleh serangan tersebut.

Sebelum melanjutkan pada kondisi PC. Dalam penelitian ini akan menggunakan spesifikasi PC *server*, dimana sistem oprasinya menggunakan Windows xp, prosesornya Core i3, kecepatan prosesornya 2.30 GHz dan ram 2 GB.

Dalam proses serangan DDoS yang langsung ditujukan kepada *server* terdapat *CPU usage* dalam kondisi dimana yang terlihat pada gambar 12

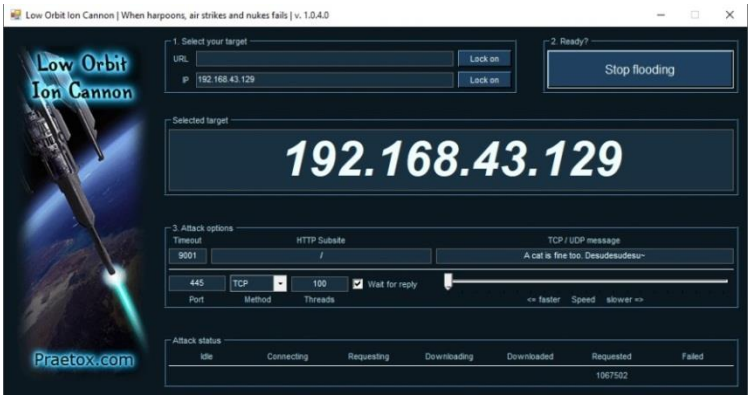


Gambar 12 Kondisi Cpu Usage

Berdasarkan gambar 12 Merupakan kondisi *server* dan *CPU usage* saat serangan DDoS (*Distributer Danial of Service*), bisa dilihat konidisi *cpu usage* hampir dipastikan mengalami peningkatan beban sebesar 50% dari kondisi normal.

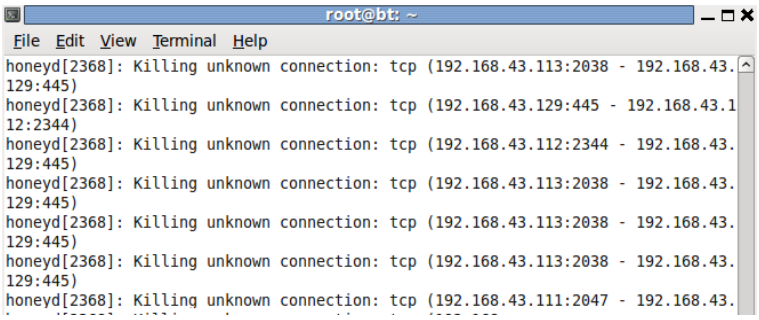
Pengujian Jaringan Akhir

Pada pengujian jaringan akhir akan dilakukan uji coba serangan DDoS dengan menggunakan *tools* LOIC (*Low Orbit Ion Cannon*), bertujuan untuk membuktikan bahwa pengujian serangan DDoS sudah terdeteksi dengan *honeyd* dan LOIC akan melakukan serangan pada *PC server* dengan perintah seperti yang terlihat di gambar 13



Gambar 13 Serangan Pada *Server*

Pada *tools* LOIC akan menyerang menggunakan perintah ip 192.168.43.129 *port* 445 *melhod* threads 1000 serta pengaturan kecepatan penyerang dengan merubah *slider* kearah *faster*.seperti terlihat pada gambar 13 setelah serangan dilancarkan maka terlebih dahulu *honeyd* akan dijalankan, berikut proses *honeyd* saat dijalankan.



Gambar 14 Aktifitas Honeyd

Pada gambar 14 merupakan atifitas *honeyd* dalam mendeteksi serangan terlihat adanya serangan dengan alamat ip 192.168.43.129 yang diserangan dengan port 445 dan alamat ip 192.168.43.113, 192.168.43.112, 192.168.43.111 adalah ip yang di gunakan *attacker* untuk menyerang, besaran paket yang di terima oleh *honeyd* setiap *and off connection* sebesar 2038 untuk ip 192.168.43.1113, 2038 untuk ip192.168.43.112 dan 2047 untuk ip 192.168.43.111. Besaran ini akan terus bertambah sampai serangannya berhenti.

Hasil Pengujian Awal

Berdasarkan hasil yang di dapat pada awal pengujian yang telah dilakukan dengan baik yang diciptakan oleh *honeyd* bahwa proses *port scanning* yang dilakukaan oleh *zenmap* terlihat bahwa *port-port* yang terbuka mampu memiliki *service-service* yang tidak nyata untuk mengelabuhi atau mengalihkan perhatian para *attacker*. kondisi *server* saat tejadi serangan DDoS (*Distributer Danial of Service*), *cpu usage* hampir dipastikan mengalami peningkatan beban sebesar 50% dari kondisi normal.

Hasil Pengujian Akhir

Hasil yang didapat pada pengujian akhir disimpulkan bahwa ketika *attacker* berinteraksi langsung ke dalam *server* yang asli maka *honeyd* mampu mendeteksi serangan DDoS (*Distributed Denial of Service*) dan memberikan informasi kepada *honeyd* berupa alamat *IP*, *port*, dan besaran paket yang diterima oleh *honeyd*.

Analisis

Dalam penelitian ini digunakan tiga *attacker* yang digunakan untuk menyerang *server*, dari penyerangan DDoS tersebut akan diketahui secara langsung dampak yang dihasilkan pada *server* dan mendeteksi serangan akan digunakan *honeyd* agar serangan-serangan DDoS tersebut terdeteksi, untuk membuktikan hasil dari serangan akan dilakukan percobaan sebanyak 10 kali percobaan serangan dan untuk memudahkan dalam membaca jumlah paket yang diterima oleh *honyed* maka akan ditunjukan seperti pada tabel 1.

Tabel 1 Jumlah Paket

Pengujian	Alamat IP		
	192.168.43.111	192.168.43.112	192.168.43.113
1	1681	1542	1494
2	1373	1978	1891
3	1954	1493	1891
4	2657	2494	2391
5	1734	1931	1415
6	2478	2302	2861
7	1208	1398	1642
8	2871	2603	2143
9	1214	1441	1973
10	2038	2047	2038

END OFF

Berdasarkan tambel 1 pengujian dikakukan sebanyak 10 kali percobaan, terdapat alamat IP mulai dari 192.168.43.111, 192.168.43.112, dan 192.168.43.113 yang melakukan penyerangan dan besaran paket yang diterima oleh *honeyd* setiap *and off connection* berbeda-beda pada 10 kali percobaan. Dengan demikian bisa di pastikan bahwa ketiga alamat IP tersebut digunakan *attacker* untuk menyerang *server*.

Terbukti *honeyd* mampu menyerupai sistem aslinya yang berpura-pura memiliki *service-service* yang tidak nyata, akan tetapi ketika *honeyd* tidak bisa mengecoh serangan dengan berpura-pura sebagai *server* dan langsung menyerang *server* yang asli. Yang terjadi, *honeyd* juga mampu mendeteksi serangan secara *real time* dan memberikan informasi dari aktifitas berupa status penyerang yang telah diproleh oleh *honeyd*.

KESIMPULAN

Pada kesimpulan seputar penelitian yang telah dilakukan berdasarkan pada perancangan dan implementasi sistem keamanan jaringan menggunakan *honeypot* dengan melakukan tahap uji coba dan dapat ditarik kesimpulan sebagai berikut :

1. *Honeypot* dapat mengemulasikan *virtual host* dan memberikan servis yang mirip dengan komputer aslinya kepada *attacker*.

2. Dengan didapatkannya status penyerang yang di hasilkan oleh sistem *honeypot*, admin dapat mengetahui informasi-informasi penyerang yang terjadi pada *server*, sehingga kedepannya admin dapat menutupi celah-celah untuk kemungkinan target penyerangan kedepannya.
3. Dengan sistem keamanan jaringan *honeypot* dapat membantu mendeteksi serangan-serangan DDoS secara *real time*.

SARAN

Honeypot merupakan aplikasi yang bisa terus berkembang demi terciptanya sebuah sistem yang lebih baik lagi, dan untuk pengembangan pembangunan sistem keamanan *honeypot* kedepannya, ada beberapa saran yang dapat dijadikan pertimbangan diantaranya :

1. Banyak aplikasi *honeypot* dengan jenis yang berbeda dan dengan kemampuan kemampuan yang berbeda pula sehingga dalam penelitian dapat memilih aplikasi yang diinginkan.
2. Untuk pengembangan kedepannya dianjurkan menggunakan notifikasi sebagai pemberitahuan jika terjadi serangan DDoS.

DAFTAR PUSTAKA

Aidin, L., Nasution, S., dan Azmi, F. (2016). "Implementasi High Interaction *Honeypot* Pada *Server*". *E-Proceeding of Engineering* Vol. 3. No. (2). 2172-2178

Fathoni, W., Fitryani, Nurkahfi, G. (2016). "Deteksi Penyusup Pada Jaringan Komputer Menggunakan IDS *SNORT*". *E-Proceeding of Engineering* Vol. 3. No. (1). 1169-1172

Ferdiansyah, D. (2013). "Pemanfaatan Teknologi Honeypot Dalam Meningkatkan *Evailability* Pada Sistem Jaringan". *Jurnal Informatika Manajemen dan Teknologi* Vol. 15. No. (1). 11-18

Jain, A., Singh, A. (2012) "*Distributed Denial Of Service (DDOS) Attack – Classification and Implications*". *Jurnal Of Information Operations Management* Vol. 3. No. (1). 136-140

Masse, F., Hidayat, A., dan Badrianto. (2015) "Penerapan *Network Intrusion Detection System* Menggunakan *Snort* Berbasis *Database* Myaql Pada *Hotspot* Kota". *Jurnal Elektronik Sistem Informasi dan Komputer* Vol. 1. No. (2). 1-16

Micro, A. (2012). "Dasar-Dasar Jaringan Komputer*"*. [online]. Tersedia: http://clearos-indonesia.com [12 Desember 2018]

Nayyar, R., Harshita. (2017). "*Identification of DoS Attack on Web Server*". Vol. 5. No. (2). 206-210

Sutarti, Khairunnisa. (2017). "Perancangan dan Analisis Keamanan Jaringan Nirkabel Dari Serangan DDoS (*Distributed Denial of Service*) Berbasis *Honeypot". Jurnal Prosisko* Vol. 4. No. (2). 9-16

Tambunan, B.,Raharjo,W., Purwadi, J. (2013). "Desain Dan Implementsi *Honeypot* Dengan *Fwsnort* Dan PSAD Sebagai *Intrusion Prevention System*". *Ultima Computing* Vol. 5. No. (1). 1-7

Utdirartatmo, f. (2005). "Trik Menjebak *Hacker* Dengan *Honeypot*". Yogyakarta. Andi.

Wilman, Fitri, I., Nathasia. (2018). "*Port Knocking* dan Honeypot Sebagai Keamanan Jaringan Pada *Server Ubuntu Virtual". Jurnal Informatika Merdeka Pasuruan* Vol. 3. No. (1). 27-33