PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET

SKRIPSI

Disusun Oleh :

SETYO WARDOYO
09.18.124

JURUSAN TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2013

LEMBAR PERSETUJUAN

PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET

SKRIPSI

Disusun dan diajukan untuk melengkapi dan memenuhi persyaratan guna mencapai gelar Sarjana Teknik

Disusun Oleh :

SETYO WARDOYO

09.18.124

Diperiksa dan disetujui,

Dosen Pembimbing 1	Dosen Pembmbing II
Joseph Dedy Irawan, ST. MT	**Sonny Prasetio, ST, MT.**
NIP. 19740416 200501 1 002	**NIP.P. 1031000433**

Mengetahui,
Ketua Program Studi Teknik Informatika S-1

Joseph Dedy Irawan, ST. MT
NIP. 19740416 200501 1 002

JURUSAN TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2013

PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL
MALANG

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	:	SetyoWardoyo
Nim	:	09.18.124
Program Studi	:	Teknik Informatika S-1
Fakultas	:	Teknologi Industri

Menyatakan dengan sesungguhnya bahwa Skripsi saya yang berjudul:
"PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET"
Adalah hasil karya sendiri bukan hasil karya orang lain, kecuali kutipan yang telah saya sebutkan sumbernya

Malang, 12 Agustus 2013
Yang membuat pernyataan

METERAI TEMPEL
6000 DJP

Setyo Wardoyo

INTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
PROGRAM STUDI TEKNIK INFORMATIKA S-1
Jl. Karanglo Km. 2 Malang

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

Nama : Setyo Wardoyo
NIM : 0918124
Jurusan : Teknik Informatika S-1
Judul : Perancangan Aplikasi Analisis Deteksi Keamanan Jaringan Menggunakan Honeypot Dionaea Pada Jaringan Internet

Dipertahankan dihadapan Majelis Penguji Skripsi Jenjang Strata Satu (S-1) pada :
Hari : Kamis
Tanggal : 15 Agustus 2013
Nilai : 82.37 (A)

Panitia Ujian Skripsi :

Ketua Majelis Penguji

Joseph Dedy Irawan, ST, MT
NIP.19740416 200501 1 002

Anggota Penguji :

Penguji Pertama

Ali Mahmudi, BEng, PhD
NIP.P. 1031000429

Penguji Kedua

Yosep Agus Pranoto,ST
NIP.P. 1031000432

INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
PROGRAM STUDI TEKNIK INFORMATIKA S-1
Jl. Karanglo, KM 2 Malang

FORMULIR PERBAIKAN SKRIPSI

Dalam pelaksanaan ujian skripsi jenjang Strata 1 Program Studi Teknik Informatika, maka perlu adanya perbaikan skripsi untuk mahasiswa :

NAMA : Setyo Wardoyo
NIM : 0918124
JURUSAN : Teknik Informatika S-1
JUDUL : **PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET**

No	Penguji	Tanggal	Uraian	Paraf
1.	Penguji I	15 Agustus 2013	1. Hal 20&21 terlalu banyak yang kosong 2. Daftar Pustaka harus ada yang dari buku,jurnal atau ebook 3. Perbaiki refrensi BAB 1 dan 2 harus ada dasar refrensi di daftar pustaka 4. Ada gambar double di hal 34&35 5. Hal 43&44 ada double langkah 6. Batasan masalah no 5 7. Demo jika ada serangan , muncl notif	
2.	Penguji II	15 Agustus 2013	1. Perbaiki format penulisan 2. Perbaiki flowchart Gambar 3.2 3. Perbaiki batasan masalah 4. Perbaiki kesimpulan dan sarapn 5. Muncul notif jika ada serangan	

Anggota Penguji

Penguji Pertama

Ali Mahmudi, BEng, PhD
NIP.P. 1031000429

Penguji Kedua

Yosep Agus Pranoto,ST
NIP.P. 1031000432

Mengetahui

Dosen Pembimbing I

Joseph Dedy Irawan, ST, MT
NIP.19740416 200501 1 002

Dosen Pembimbing II

Sonny Prasetio, ST, MT
NIP.P.1031000433

PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET

SETYO WARDOYO
0918124
Program Studi Teknik Informatika S-1

Fakultas Teknologi Industri
Institut Teknologi Nasional Malang
Email : thekillerdoll@gmail.com

Dosen Pembimbing : 1. Yoseph Dedy Irawan, ST, MT.
2. Bapak Sonny Prasetio, ST, MT.,

Keamanan sistem informasi berbasis Internet harus sangat diperhatikan, karena jaringan komputer Internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam Internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada user Internet yang lain untuk menyadap atau mengubah data tersebut. Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif.

Honeypot adalah suatu sistem yang didesain menyerupai sistem asli dan dibuat dengan tujuan untuk diserang. Karena honeypot bukan merupakan sistem asli, maka hanya sedikit atau bahkan tidak ada sama sekali trafik jaringan yang berasal dari atau menuju honeypot. Oleh karena itu, semua trafik honeypot patut dicurigai sebagai fasilitas yang tidak sah. Hal itu memungkinkan untuk melakukan pendeteksian dan menganalisa terhadap usaha – usaha tersebut dengan cara melakukan pengawasan terhadap honeypot.

Sistem honeypot dionaea memberikan hasil sebesar 92 % pada tingkat keberhasilan sistem, 8 % gagal pengujian dalam pendeteksian malware dari sebuah attacker PC

Kata kunci : Honeypot, Dionaea, Malware, keamanan jaringan,penyusup

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Tuhan Yang Maha Esa, karena atas rahmat dan hidayahnya sehingga penulis dapat menyelesaikan Laporan Skripsi yang berudul "**PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET**" ini dengan baik.

Laporan Skripsi ini merupakan salah satu persyaratan akademik yang harus dipenuhi oleh mahasiswa Institut Teknologi Nasional Malang untuk memperoleh gelar Strata 1 Program Studi Teknik Informatika, Institut Teknologi Nasional Malang.

Oleh karena itu, pada kesempatan ini dengan segala kerendahan hati perkenankanlah penulis mengucapkan terimah kasih kepada :

1. **Tuhan Yang Maha Esa**, yang senantiasa memberikan kesehatan kepada penulis sehingga dapat menyelesaikan Laporan Skripsi ini dengan baik.
2. **Kedua Orang Tua**, serta keluarga yang sentiasa memberikan dorongan baik secara Moril maupun Materiel dalam menyelesaikan Laporan Skripsi ini.
3. **Bapak Ir. Soeparno Djiwo, MT.**,selaku Rektor Institut Teknologi Nasional Malang.
4. **Bapak Yoseph Dedy Irawan, ST, MT.**,selaku Ketua Jurusan Teknik Informatika S-1 Institut Teknologi Nasional Malang.
5. **Bapak Yoseph Dedy Irawan, ST, MT.**, selaku Dosen Pembimbing I Program Studi Teknik Informatika S-1 Institut Teknologi Nasional Malang.
6. **Bapak Sonny Prasetio, ST, MT.**, selaku Dosen Pembimbing II Program Studi Teknik Informatika S-1 Institut Teknologi Nasional Malang.
7. Serta semua pihak yang telah membantu dalam menyelesaikan Laporan Skripsi ini baik secara langsung maupun tidak langsung,

sehingga penulis dapat menyelesaikan Laporan Skripsi ini dengan baik.

Penulis menyadari Laporan Skripsi ini masih jauh dari kesempurnaan, oleh karena itu penulis mengharap kritik dan saran yang bersifat membangun dari semua pihak guna sempurnanya Laporan Skripsi ini.

Akhir kata penulis mohon maaf yang sebesar-besarnya bila mana dalam penyusunan Laporan Skripsiini terdapat kekurangan serta kesalahan. Semoga Laporan Skripsi ini dapat bermanfaat bagi kita semua.

Malang, Juli 2013

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1. 1 Latar Belakang

Keamanan sistem informasi berbasis Internet harus sangat diperhatikan, karena jaringan komputer *Internet* yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam Internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada *user* Internet yang lain untuk menyadap atau mengubah data tersebut. Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif.

Honeypot adalah suatu sistem yang didesain menyerupai sistem asli dan dibuat dengan tujuan untuk diserang. Karena *honeypot* bukan merupakan sistem asli, maka hanya sedikit atau bahkan tidak ada sama sekali *trafik* jaringan yang berasal dari *honeypot* maupun menuju *honeypot*. Oleh karena itu, semua *trafik honeypot* patut dicurigai sebagai fasilitas yang tidak sah. Hal itu memungkinkan untuk melakukan pendeteksian dan menganalisa terhadap usaha – usaha tersebut dengan cara melakukan pengawasan terhadap *honeypot*.

Pada skripsi penulis ini berkaitan dengan pengimplementasian *honeypot* dengan *Wireless LAN* atau *LAN*. Impelementasi *honeypot* ini diletakan pada jaringan *internet* menggunakan ip publik, yang fungsinya untuk mengobservasi *malware* yang masuk pada jaringan. Sehingga *administrator* hanya menunggu serangan yang datang menuju *honeypot*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, bagaimana cara melakukan implementasi *honeypot* dalam mendeteksi dan analisa *malware* dengan menggunakan dionaea, dan bagaimana cara pengujian *honeypot* di jaringan *internet*.

1.6 Sistematika Penulisan

Sistematika penyusunan proposal ditujukan untuk memberikan gambaran dan uraian dari proposal skirpsi secara garis besar yang meliputi bab-bab sebagai berikut :

BAB I : PENDAHULUAN

Pada Bab ini membahas tentang Latar Belakang, Rumusan Masalah, Batasan Masalah, Maksud dan Tujuan Penelitian, Manfaat Penelitian, Metode Penelitian dan Sistematika Penulisan Laporan Penelitian.

BAB II : LANDASAN TEORI

Pada Bab ini membahas tentang Landasan Teori yang merupakan tinjauan pustaka, menguraikan teori-teori yang mendukung judul, dan pembahasan secara detail. Landasan teori dapat berupa definisi-definisi atau model yang langsung berkaitan dengan ilmu atau masalah yang diteliti. Pada bab ini juga dituliskan tentang software (komponen) yang digunakan dalam pembuatan Program atau keperluan saat penelitian.

BAB III: ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi antara lain: Tinjauan Umum yang menguraikan tentang gambaran umum objek penelitian, misalnya gambaran umum Instansi (struktur organisasi, Pengelolaan dll, serta data yang dipergunakan untuk memecahkan masalah-masalah yang dihadapi, berkaitan dengan kegiatan penelitian.

Pada Bab ini juga membahas "analisis masalah", yang akan menguraikan tentang analisis terhadap permasalahan yang terdapat pada kasus yang sedang di teliti. Meliputi analisis terhadap masalah sistem yang sedang berjalan, analisis hasil solusinya, dan analisis kebutuhan penelitian.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Pada Bab ini akan membahas paparan implementasi dan analisis hasil uji coba program, serta memaparkan hasil-hasil dari tahapan penelitian, dari tahap analisis,

desain, implementasi desain, hasil testing dan implementasinya, berupa penjelasan teoritik, baik secara kualitatif, kuantitatif, atau secara statistik. Dan Selain membandingkan dengan hasil penelitian yang masih manual.

BAB V : PENUTUP

Pada Bab ini berisi kesimpulan dan saran. Kesimpulan didapat dari ulasan data – data penelitian, menyimpulkan bukti-bukti yang diperoleh dan akhirnya menarik intisari apakah hasil yang didapat (dikerjakan), layak untuk digunakan (diimplementasikan).

BAB II
LANDASAN TEORI

2.1 *HONEYPOT* [6]

Honeypot merupakan sebuah sistem komputer yang sengaja "dikorbankan" untuk menjadi target serangan dari *hacker*. Komputer tersebut melayani setiap serangan yang dilakukan oleh *hacker* dalam melakukan penetrasi terhadap server tersebut. Metode ini ditujukan agar *administrator* dari server yang akan diserang dapat mengetahui trik penetrasi yang dilakukan *hacker* serta bisa melakukan antisipasi dalam melindungi server yang sesungguhnya. Setiap tindakan yang dilakukan oleh penyusup yang mencoba melakukan koneksi ke *honeypot* tersebut, maka *honeypot* akan mendeteksi dan mencatatnya.

Perlu diingat bahwa peran dari *honeypot* bukanlah menyelesaikan suatu masalah yang akan dihadapi server, akan tetapi memiliki kontribusi dalam hal keseluruhan keamanan. Dan besarnya kontribusi tersebut tergantung dari bagaimana kita menggunakannya. Intinya, walaupun tidak secara langsung melakukan pencegahan terhadap serangan (*firewall*) tetapi dapat mengurangi dari intensitas serangan yang akan dilakukan oleh penyusup ke server yang sesungguhnya

2.2 TIPE *HONEYPOT* [7]

Honeypot dapat dibagi menjadi dua tipe dasar, yaitu *production honeypot* dan *research honeypot*. Tujuan utama dari production *honeypot* adalah untuk membantu mengurangi resiko keamanan jaringan pada sebuah sistem. Production *honeypot* memberikan suatu nilai tambah bagi keamanan jaringan dari suatu sistem. Tipe kedua, research *honeypot*, adalah *honeypot* yang didesain untuk mendapatkan informasi mengenai aktivitas – aktivitas dari komunitas penyerang atau penyusup. Research *honeypot* tidak memberikan suatu nilai tambah secara langsung kepada suatu sistem, melainkan digunakan sebagai alat untuk meneliti ancaman - ancaman keamanan yang mungkin dihadapi dan bagaimana cara untuk melindungi diri dari ancaman tersebut.

– batasan tersebut, maka tingkat risiko yang dihadapi semakin tinggi karena penyerang dapat memiliki akses root. Pada saat yang sama, kemungkinan pengumpulan informasi semakin meningkat dikarenakan kemungkinan serangan yang tinggi. Dikarenakan penyerang dapat berinteraksi secara penuh dengan sistem operasi, maka apabila ia telah mendapat akses root ia dapat meng-upload dan meng-install file – file baru. Apabila hal tersebut terjadi maka dimungkinkan untuk memperoleh informasi – informasi baru mengenai komunitas *blackhat*. Informasi tersebut dapat berupa pola serangan, toolkit yang digunakan, motivasi dan lain – lain. Disinilah letak kelebihan dari high – interaction *honeypot*. Hanya saja high – interaction *honeypot* menghabiskan banyak waktu karena harus diawasi secara kontinu. Pengawasan ini diperlukan karena apabila *high – interaction honeypot* telah diambil alih dan dimanfaatkan oleh penyerang maka *honeypot* tersebut dapat menjadi ancaman bagi jaringan yang ada.

2.4 Nilai guna *Honeypot* [7]

Secara umum, keamanan jaringan dapat dibagi menjadi tiga area, sebagaimana yang didefinisikan oleh Bruce Schneier sebagai berikut:

1. *Prevention* (pencegahan)
2. *Detection* (pendeteksian)
3. *Reaction* (reaksi)

Berikut ini, akan dijelaskan fungsi *honeypot* di dalam tiga area keamanan jaringan yaitu prevention, detection dan reaction.

2.4.1. Prevention

Salah satu idc yang digunakan pada area *prevention* (pencegahan) adalah menggunakan *honeypot* sebagai pengalih perhatian untuk mencegah terjadinya serangan. Konsep utama yang terdapat pada area ini adalah bagaimana membuat penyerang menghabiskan waktu dan sumber daya yang dimiliki untuk menyerang *honeypot* dan bukannya menyerang sistem produksi (server).

Penyerang dialihkan perhatiannya untuk menyerang *honeypot* sehingga mengurangi resiko sistem produksi (server) dari serangan. Bahkan jika penyerang

mengetahui bahwa pada jaringan tersebut terdapat sebuah *honeypot*, tetapi tidak mengetahui di mana posisi *honeypot* tersebut maka hal ini akan membingungkan penyerang. Ide utama dari konsep ini adalah pencegahan dan pengelabuan. Pada saat ini, serangan yang sering terjadi adalah serangan yang terotomatisasi seperti worm dan auto-rooter. Serangan ini biasanya terjadi secara random yang akan memindai seluruh jaringan untuk mencari sistem yang dapat ditembus (vulnerable systems). Ada beberapa *honeypot* yang didisain khusus untuk menghadapi serangan semacam ini, *honeypot* tersebut biasa disebut sebagai sticky *honeypot*. Yang dilakukan sticky *honeypot* pada serangan seperti tersebut di atas adalah memperlambat proses pemindaian yang dilakukan oleh worm dan auto-rooter. Konsep yang digunakan adalah pengembangan proses yang terjadi setelah proses 3-way handshake pada TCP selesai dilakukan.

Pengembangan yang pertama adalah mengabaikan setiap paket yang datang setelah koneksi terjalin (*3-way handshake* selesai) sampai koneksi tersebut mengalami time-out. Pengembangan kedua adalah setelah 3-way handshake selesai dan penyerang (worm) mulai mengirimkan datanya maka *sticky honeypot* akan menjawab dengan mengirimkan TCP window 0 (wait). Proses ini akan dilakukan berulang – ulang untuk menahan koneksi tersebut dan mencegah worm menyerang jaringan lain.

2.4.2. Detection

Honeypot berguna pada proses pendeteksian karena dapat menyederhanakan proses pendeteksian. Besarnya trafik jaringan yang ada pada saat ini dapat menimbulkan beban yang berlebihan pada sumber daya keamanan yang ada. Trafik yang besar tersebut harus dipilah satu persatu oleh sumber daya keamanan. Dikarenakan *honeypot* tidak memiliki aktivitas produksi, maka setiap koneksi dari dan menuju *honeypot* langsung dapat dicurigai. Secara umum, setiap koneksi yang berhubungan dengan *honeypot* dapat dikategorikan sebagai aktivitas yang tidak terotorisasi. Hal ini memudahkan di dalam pencarian dan pengumpulan informasi yang diinginkan.

2.4.3. Reaction

Walaupun secara umum jarang disebutkan, *honeypot* mempunyai kegunaan di dalam area reaction (reaksi). Kadangkala ketika sebuah sistem produksi pada sebuah sistem telah disusupi / diambil alih, aktivitas jaringan tetap saja terjadi yang mengakibatkan bukti – bukti mengenai penyusupan tersebut menjadi terkontaminasi. Seorang administrator tidak akan dapat menentukan apa yang sebenarnya terjadi pada sistem produksi ketika *user* dan aktivitas jaringan yang ada telah mengaburkan data insiden. Pengumpulan informasi akan sangat sulit dilakukan pada kasus seperti itu.

Permasalahan yang mungkin terjadi berikutnya adalah sering kali sistem produksi yang telah disusupi / diambil alih tidak bisa dilepas dari jaringan (*offline*). Adakalanya suatu layanan (*service*) yang diberikan oleh sistem produksi harus dipulihkan secepat mungkin. Kasus ini biasanya terjadi pada server yang menangani transaksi *e-commerce*. Hal ini akan menyulitkan bagi administrator di dalam melakukan analisis penuh terhadap insiden yang terjadi.

Honeypot memberikan solusi bagi kedua permasalahan tersebut di atas. Dikarenakan *honeypot* tidak memberikan suatu layanan tertentu kepada *user* maka data –data yang terkumpul biasanya merupakan data – data insiden dan kontaminasi dari aktivitas jaringan yang ada biasanya sangat sedikit. Selain itu keuntungan dari penggunaan *honeypot* adalah bila *honeypot* telah berhasil disusupi / diambil alih, maka *honeypot* dapat dilepas dari jaringan (*offline*) karena *honeypot* tidak memberikan suatu layanan tertentu yang harus segera dipulihkan.

2.5 Kelemahan Sistem Deteksi yang ada [7]

Tingginya tingkat aktivitas jaringan yang terjadi kadangkala menyebabkan sulitnya untuk mendeteksi adanya sebuah serangan atau bahkan mendeteksi apabila sebuah sistem telah diambil alih. IDS (*Intrusion Detection System*) adalah sebuah sistem yang didisain untuk mendeteksi adanya kemungkinan serangan (akses yang tidak terotorisasi) yang terjadi. Hanya saja ada dua kelemahan mendasar yang terdapat pada IDS yaitu *false positive* dan *false negative*

False positive terjadi ketika ada peringatan yang dibangkitkan oleh sensor IDS yang mengenali pola serangan yang terjadi berdasarkan suatu signature tertentu. Akan tetapi pada kenyataannya pola serangan tersebut hanyalah trafik yang sah atau serangan yang tidak mungkin terjadi pada sistem.

Permasalahannya adalah ketika administrator menerima begitu banyak peringatan yang muncul sehingga administrator tidak mampu merespons setiap peringatan tersebut. Apabila hal ini terjadi secara terus menerus, ada kecenderungan pada akhirnya administrator akan mengabaikan peringatan yang muncul. Ini mengakibatkan sistem pendeteksian yang dilakukan oleh IDS menjadi tidak efektif kecuali apabila *false positive* berhasil dikurangi. Akan tetapi tidak berarti *honeypot* tidak akan menerima *false positive*, hanya saja kemungkinan *honeypot* menerima false positive lebih sedikit bila dibandingkan dengan IDS.

False negative terjadi ketika IDS gagal untuk mendeteksi suatu serangan. Sering terjadi IDS gagal untuk mendeteksi suatu serangan baru atau serangan yang tidak dikenali. Hal ini dikarenakan serangan tersebut belum terdefinisikan di dalam intrusion signature database yang dimiliki oleh IDS. Selain itu, saat ini banyak dikembangkan metode – metode untuk menghindari IDS. *Honeypot* dapat mengurangi kemungkinan *false negative* ini karena *honeypot* melakukan deteksi bukan berdasarkan kepada *signature* akan tetapi berdasarkan kepada aktivitas jaringan yang terjadi. Apabila terdapat trafik yang menuju kepada *honeypot* atau sebaliknya maka kemungkinan besar sebuah serangan sedang terjadi. Oleh karena sistem pendeteksian *honeypot* tidak menggunakan signature, maka administrator tidak perlu meng-update secara berkala.

2.6 Skema Pengumpulan Informasi [7]

Secara umum, metode pengumpulan informasi dapat dibagi menjadi 2 (dua) kategori dasar, yaitu :

1. *Host-based Information Gathering* (pengumpulan informasi berbasis host).
2. *Network-based Information Gathering* (pengumpulan informasi berbasis network/jaringan).

2.6.1 Host-based Information Gathering

Yang dimaksud dengan *host based information gathering* adalah suatu metode untuk mengetahui apa yang sedang terjadi pada *honeypot* dengan memasang mekanisme pengumpulan informasi pada honeypot itu sendiri. Diantara yang termasuk ke dalam host based information gathering adalah :

1. *Keystroke logging*

   Adalah suatu metode untuk mencatat setiap tombol yang ditekan oleh penyerang ketika sistem telah berhasil diambil alih.

2. *Syslog*

   Adalah suatu utilitas internal yang terdapat pada sistem operasi turunan UNIX yang berfungsi untuk mencatat aktifitas sistem yang terjadi.

2.6.2 Network-based Information Gathering

Yang dimaksud dengan *network based information gathering* adalah suatu metode pengumpulan informasi untuk mengetahui apa yang sedang terjadi pada honeypot dengan memasang mekanisme pengumpulan informasi pada jaringan dimana honeypot tersebut berada untuk mengamati trafik dari jaringan. Diantara yang termasuk ke dalam *network based information gathering* adalah :

1. *Firewall log*

   Firewall adalah sistem yang didesain untuk mencegah akses yang tidak terotorisasi dari dan ke sebuah jaringan privat. *Firewall* dapat dikonfigurasi untuk merekam (log) sebagian atau seluruh paket yang melewati jaringan. Kegiatan perekaman tersebut berguna apabila paket – paket yang telah melewati jaringan akan diperiksa secara seksama.

2. *Intrusion Detection System (IDS) log*

   Intrusion Detection System (IDS) adalah sistem yang berfungsi untuk menginspeksi aktivitas jaringan (masuk dan keluar) dan mengidentifikasi pola.

   pola mencurigakan pada trafik jaringan yang ada yang mengindikasikan adanya serangan terhadap suatu sistem atau jaringan. Sebuah IDS bekerja berdasarkan pola (*signature*) yang telah didefinisikan sebelumnya. IDS

melakukan kegiatan perekaman (log) untuk mencatat aktivitas – aktivitas mencurigakan yang terjadi pada jaringan.

2.7 *Malware* [3]

Perangkat perusak (bahasa Inggris: *malware*, berasal dari kata *malicious* dan *software*) adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer tanpa izin (*informed consent*) dari pemilik. Istilah ini adalah istilah umum yang dipakai oleh pakar komputer untuk mengartikan berbagai macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik. Istilah 'virus komputer' kadang-kadang dipakai sebagai frasa pemikat (*catch phrase*) untuk mencakup semua jenis perangkat perusak, termasuk virus murni (*true virus*).

2.8 *Dionaea* [11]

Dionaea adalah perangkat lunak yang menawarkan layanan jaringan yang dapat dieksploitasi. Dalam tindakan yang dilakukan adalah untuk menjebak atau mengekploitasi *Malware* yang menyerang jaringan, tujuan utamanya adalah mendapatkan salinan *malware*.

Penyerang biasanya berkomunikasi dengan beberapa service dengan mengirimkan beberapa paket terlebih dahulu kemudian mengirimkan payload. Dionaea memiliki kemampuan untuk mendeteksi dan mengevaluasi *payload* tersebut untuk dapat memperoleh salinan copy dari *malware*. Untuk melakukannya, *Dionaea* menggunakan *libemu*.Setelah *Dionaea* memperoleh lokasi file yang diinginkan penyerang/attacker untuk didownload dari shellcode, Dionaea akan mencoba untuk mendownload file.Setelah Dionaea mendapat salinan dari *worm attacker*, *Dionaea* akan menyimpan file lokal untuk analisa lebih lanjut, atau mengirimkan file ke beberapa pihak ke-3 untuk analisis lebih lanjut.

2.9 Python [1]

Python adalah bahasa pemprograman *interpretatif* multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. *Python* diklaim sebagai bahasa yang menggabungkan kapabilitas, kemampuan, dengan sintaksis kode yang sangat jelas, dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif.

Python mendukung multi paradigma pemrograman, utamanya; namun tidak dibatasi; pada pemrograman berorientasi objek, pemrograman *imperatif*, dan pemrograman fungsional. Salah satu fitur yang tersedia pada *python* adalah sebagai bahasa pemrograman dinamis yang dilengkapi dengan manajemen memori otomatis. Seperti halnya pada bahasa pemrograman dinamis lainnya, *python* umumnya digunakan sebagai bahasa skrip meski pada praktiknya penggunaan bahasa ini lebih luas mencakup konteks pemanfaatan yang umumnya tidak dilakukan dengan menggunakan bahasa skrip. *Python* dapat digunakan untuk berbagai keperluan pengembangan perangkat lunak dan dapat berjalan di berbagai *platform* sistem operasi.

Saat ini kode *python* dapat dijalankan di berbagai *platform* sistem operasi, beberapa diantaranya dalah:

1. Linux/Unix
2. Windows
3. Mac OS X
4. Java Virtual Machine
5. OS/2
6. Amiga
7. Palm
8. Symbian (untuk produk-produk Nokia)

2.10 VPS (Virtual Privat Server) [5]

VPS (*Virtual Private Server*) adalah sebuah terobosan paling canggih dalam teknologi

Virtualisasi server. VPS adalah sebuah *physical server* yang dibagi menjadi beberapa virtual private sever. Setiap VPS terlihat dan bekerja seperti sebuah jaringan server sistem yang sebenarnya, komplit vps dengan pengaturan sendiri untuk *init script*, *users*, pemrosesan, filesistem, dan sebagainya.

VPS bekerja seperti sebuah server yang terpisah

1. VPS memiliki *processes, users*, files dan menyediakan *full root access*
2. Setiap VPS mempunyai *ip address, port number, tables, filtering* dan *routing rules* sendiri.
3. VPS dapat melakukan konfigurasi file untuk sistem dan aplikasi software
4. Setiap VPS dapat memiliki sistem *libraries* atau mengubah menjadi salah satu sistem libraries yang lain.
5. Setiap VPS dapat *delete, add, modify file* apa saja, termasuk file yang ada di dalam root, dan menginstall software aplikasi sendiri atau *mengkonfigurasi root application software*.

2.11 NAT (*Network Address Translation*) [8]

NAT (*Network Address Translation*) atau Penafsiran alamat jaringan adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (*security*), dan kemudahan serta fleksibilitas dalam administrasi jaringan.

NAT merupakan salah satu protocol dalam suatu sistem jaringan, NAT memungkinkan suatu jaringan dengan ip atau internet *protocol* yang bersifat privat atau privat ip yang sifatnya belum teregistrasi di jaringan internet untuk mengakses jalur internet, hal ini berarti suatu alamat ip dapat mengakses internet dengan menggunakan ip privat atau bukan menggunakan *ip public*, NAT biasanya dibenamkan dalam sebuah *router*, NAT juga sering digunakan untuk menggabungkan atau menghubungkan dua jaringan yang berbeda, dan mentranslate atau menterjemahkan ip privat atau bukan *ip public* dalam jaringan

internal ke dalam jaringan yang *legal network* sehingga memiliki hak untuk melakukan akses data dalam sebuah jaringan.

2.11.1 Tipe - Tipe NAT

NAT atau Network Address Translation memiliki dua tipe, yaitu :

1. NAT Tipe Statis
2. NAT Tipe Dinamis

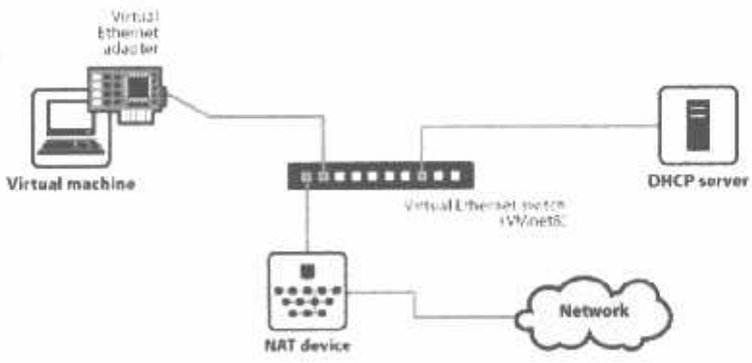
Static NAT atau NAT statis menggunakan table routing yang tetap, atau alokasi translasi alamat ip ditetapkan sesuai dengan alamat asal atau source ke alamat tujuan atau destination, sehingga tidak memungkinkan terjadinya pertukaran data dalam suatu alamat ip bila translasi alamat ipnya belum didaftarkan dalam table nat. Translasi Static terjadi ketika sebuah alamat lokal (*inside*) di petakan ke sebuah alamat global/internet (*outside*). Alamat local dan global dipetakan satu lawan satu secara statik. NAT secara statis akan melakukan request atau pengambilan dan pengiriman paket data sesuai dengan aturan yang telah ditabelkan dalam sebuah NAT .

NAT dengan tipe dinamis menggunakan logika balancing atau menggunakan logika pengaturan beban, di mana dalam tabelnya sendiri telah ditanamkan logika kemungkinan dan pemecahannya, NAT dengan tipe dinamis pada umumnya dibagi menjadi 2 jenis yaitu NAT sistem pool dan NAT sistem *overload*.

NAT dengan sistem pool atau kelompok menggunakan sebuah tabel NAT dengan logika dinamis, dimana logika yang ditanamkan dalam NAT tersebut pada umumnya merupakan logika *Fuzzy* atau jika lambang yang nilai translasinya belum pasti, dimana dalam sistem pool, suatu request belum tentu akan melewati jaringan yang sama bila melakukan request yang sama untuk kedua kalinya, Translasi Dinamik terjadi ketika *router* NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (pool) alamat global yang akan digunakan untuk terhubung ke internet. NAT dengan sistem pool biasanya sering

dimanfaatkan untuk melakukan balancing atau penyeimbangan beban pada jaringan.

NAT dengan sistem *Overloading* menggunakan logika dimana request atau permintaan dari banyak client atau banyak alamat dioperkan atau diberikan ke satu alamat ip distribusi. Sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global/outside. Sejumlah IPlokal/internal dapat ditranslasikan ke satu alamat IP global/outside. Hal ini sangat menghemat penggunakan alokasi IP dari ISP. Sharing/pemakaian bersama satu alamat IP ini menghemat penggunaan alokasi IP dari ISP. Sharing/pemakaian bersama satu alamat IP ini menggunakan metoda *portmultiplexing*, atau perubahan *port* ke *packet outbound*. Penggabungan sistem overloading dan sistem pool telah dilakukan oleh banyak produsen router dan menghasilkan logika yang banyak digunakan untuk *load balancing* saat ini yaitu *Round Robbin Load Balancing*, dimana logika ini melakukan pengiriman request secara berurutan, secara bergantian ke alamat *gateway* yang telah ditanamkan dalam tabel NAT sebelumnya, sehingga suatu *multireuest* dari sebuah alamat ip dapat melalui lebih dari satu alamat distribusi, penerapan ini dapat dilakukan dalam penggunaan *DualWan Router*, selain itu logika ini juga memiliki logika *Fail Over*, dimana bila suatu alamat distribusi tidak dapat lagi mengirimkan paket maka paket akan dialihkan ke alamat distribusi yang lain.



Gambar 2.1 jaringan dengan menggunakan alamat IP komputer host.

Koneksi terjemahan alamat jaringan sudah diatur secara otomatis jika anda mengikuti jalan Kustom di *New Virtual Machine Wizard* dan pilih gunakan terjemahan alamat jaringan.

Jika anda ingin terhubung ke *Internet* atau jaringan TCP / IP lain yang menggunakan jaringan dial-up komputer host atau koneksi *broadband* dan anda tidak mampu memberikan mesin virtual Anda alamat IP pada jaringan eksternal, NAT scring cara termudah untuk memberikan akses mesin virtual ke jaringan tersebut.

NAT juga memungkinkan Anda untuk terhubung ke jaringan TCP / IP menggunakan adaptor Cincin Token pada komputer host.

2.12 *Web Server* [4]

Web server adalah sebuah bentuk server yang khusus digunakan untuk menyimpan halaman website atau homepage Komputer dapat dikatakan web server jika komputer tersebut memiliki suatu program server yang disebut *Personal Web Server* (PWS).

Macam-macam web server antara lain :

1. Apache (*open source*)
2. Xitami
3. Iis
4. PWS (*Personal web Server*)

Website (Situs Web) merupakan alamat (URL) yang berfungsi sebagai tempat penyimpanan data dan informasi dengan berdasarkan topik tertentu situs atau web dapat dikategorikan menjadi dua yaitu :

1. Web statis

   Web yang berisi atau menampilkan informasi-informasi yang sifatnya statis (tetap)
2. Web Dinamis

   Web yang menampilkan informasi serta dapat berinteraksi dengan *user* yang bersifat dinamis.

2.13 HTTP (*Hypertext Transfer Protocol*) [2]

HTTP (*Hypertext Transfer Protocol*) merupakan protokol yang digunakan untuk mendistribusikan sistem informasi yang berbasis *hypertext*. Protokol ini merupakan protokol standar yang digunakan untuk mengakses HTML.HTTP diprakarsai oleh World Wide Web sistem informasi yang menyeluruh sejak tahun 1990. Apabila pada penjelajahan web dan pada alamat tertulis *http://www.google.com* ini merupakan salah satu penggunaan protokol HTTP dalam web.

2.14 Nmap [9]

Nmap adalah tools pemetaan jaringan (network) terbaik yang pernah ada sejauh ini. Panggunaannya yang praktis, konfigurasi yang mudah, dan kehandalannya dalam memetakan jaringan komputer di manapun. Dengan Nmap, anda dapat mengetahui komputer-komputer (hosts) apa saja yang sedang terhubung dalam sebuah jaringan, apa service (aplikasi) yang sedang dijalankan komputer itu (host), apa sistem operasi komputer yang dipakai, apa tipe firewall yang digunakan, dan karakteristik lainnya dari komputer.

Nmap juga merupakan utilitas keamanan *open-source* yang powerfull yang dapat digunakan untuk mengaudit keamanan dan mengeksplorasi jaringan, tetapi dapat juga digunakan untuk komputer yang tidak terhubung dengan jaringan. Nmap didesain untuk melakukan scanning jaringan besar atau kecil dengan menggunakan paket raw IP untuk mengetahui host yang 'up' dalam jaringan, service yang dijalankan dan nomor port yang terbuka, dan tipe *packet-filter/firewall* yang digunakan dan berbagai macam karakteristik lainnya. Nmap dapat digunakan untuk melakukan *fingerprinting* yang bisa membandingkan dan memberikan estimasi jenis sistem operasi (OS) apa yang digunakan target. Nmap juga mempunyai banyak kelebihan atau Flags yang akan memanipulasi cara Scanning. Nmap kompatibel dengan Linux/BSD Family (*nix) dan Windows.

2.15 Putty [18]

Putty adalah software *remote console/* terminal yang digunakan untuk meremote komputer dengan terhubungnya menggunakan port ssh atau sebagainya, Pada bahasan disini diterang cara untuk meremote sistem operasi linux dengan menggunakan sistem operasi windows tentunya *putty* disini diinstall diwindows jadi digunakan *putty* versi windows.

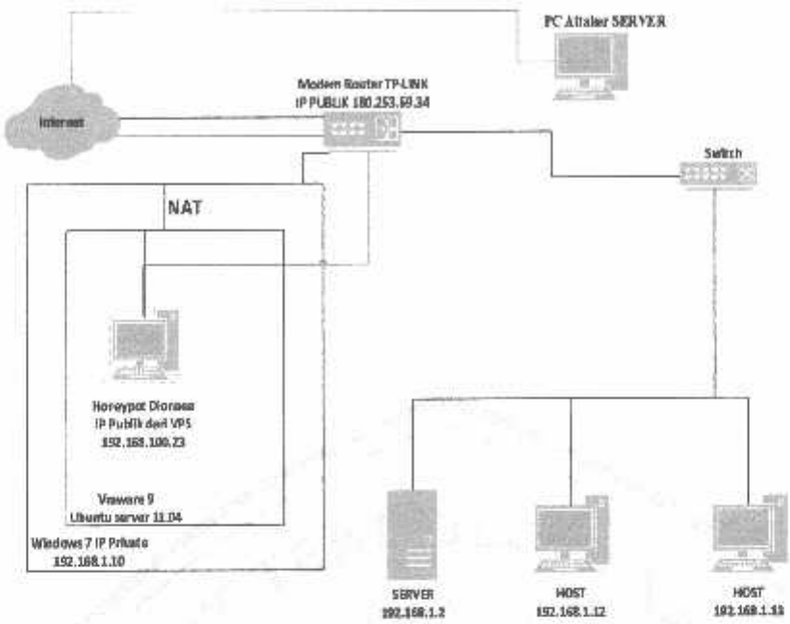
BAB III
HONEYPOT PADA JARINGAN KOMPUTER

3.1 Analisis Sistem

Sistem *honeypot dionaea* diimplementasikan pada sebuah *notebook TOSHIBA M505* dengan sistem operasi *linux Ubuntu server 11.04*, yang dikembangakan menggunakan *vmware 9*. Tujuan dari perancangan sistem ini adalah mendapatkan salinan *malware*, yaitu dengan melakukan perancangan sistem, untuk membandingkan *malware* yang tertangkap oleh *honeypot dionaea*. Dan dari hasil *malware* yang tertangkap dalam bentuk kode *binaries*, nantinya akan di *Link* ke situs anubis secara random. Sehingga dapat mengetahui jenis aplikasi yang diserang oleh virus *malware*, terindentifikasi dan tercatat secara jelas dalam bentuk file seperti HTML, XML, PDF, Text.

3.2 Lokasi Penempatan *Honeypot*

Sebuah *honeypot* tidak membutuhkan suatu lingkungan khusus, karena pada dasarnya sebuah *honeypot* tidak memberikan suatu layanan tertentu kepada pengguna, dalam artian hanya bisa di akses oleh admin yang bertanggung jawab untuk menjaga keamanan suatu sistem dari serangan *malware*. Sebuah *honeypot* dapat ditempatkan di setiap tempat di mana sebuah server ditempatkan. Meski demikian, beberapa lokasi penempatan mempunyai nilai yang lebih baik dibandingkan dengan lokasi penempatan yang lain. Pada umumnya *honeypot* akan ditempatkan di belakang gateway (dekat dengan jaringan privat (intranet)), karena ketika *hacker* akan menembus server dibelakang gateway akan tertangkap ke dalam sebuah sistem server virtual yang ada didalam *VMware 9* yang menggunakan operasi sistem ubuntu server 11.04 dan sudah terinstal *honeypot dionaea*, untuk mendeteksi sebuah perangkat lunak yang tidak wajar (*malware*). Sehingga akan menyimpan sebuah file dari aktifitas penyusup yang masuk kedalam *Honeypot Dionaea* kedalam *folder* yang sediakan oleh *honeypot dieonaea*.



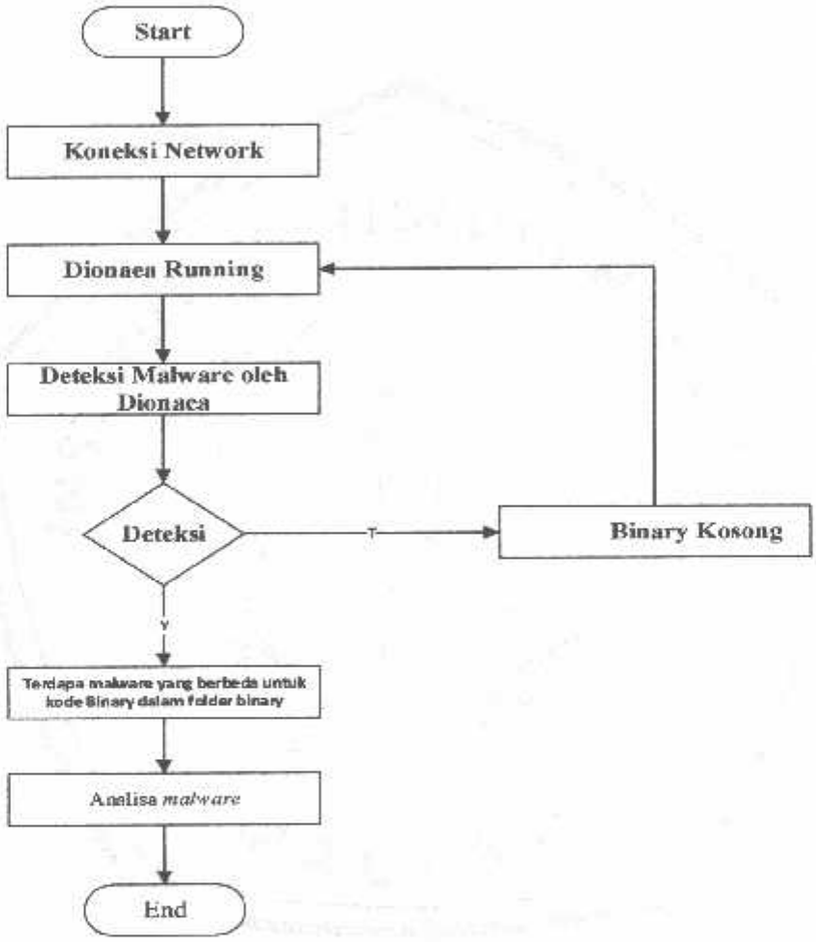
Gambar 3.1 Prediksi lokasi penempatan *Honeypot*

Gambar 3.1 menunjukan, setiap *honeypot* menggunakan IP statis. Maka dengan itu, menggunakan *virtual private server* untuk mendapatkan IP publik yang sifatnya statis, sehingga *virtual private server* tersebut didapatkan dari hasil NAT yang di konfigurasi pada *VMware 9*, sehingga mendapatkan IP publik. Ketika PC *Attacker* akan masuk kedalam jaringan, menyerang server utama, akan terjebak kedalam Ubuntu server 11.04 yang sudah terinstall *honeypot dionaea* yang ada didalam *VMware 9*. PC *Attacker* telah masuk kedalam sebuah virtual Ubuntu server 11.04, disebabkan karena operasi sistem yang penulis yang telah dirancang pada port - port tertentu disengaja dibuka agar PC *Attacker* masuk kedalam jebakan di *honeypot* yang ada didalam operasi sistem Ubuntu server 11.04 di VMware 9.

3.3 Flow Chart

Implementasi sistem *honeypot dionaea* dijalankan secara sistematis. Pada saat sistem dijalankan dan terkoneksi dengan jaringan internet, maka *dionaea* akan bekerja langsung untuk mendeteksi kemungkinan adanya program *malware* yang masuk ke dalam jaringan internet penulis. Jika terdapat *malware* yang masuk

ke dalam jaringan internet penulis, maka *dionaea* akan menyimpan sebuah data *binary* ke dalam *folder* yang telah ditentukan. Kemudian *malware* tersebut akan dideteksi dan disimpan sampai prosesnya selesai. Jika tidak terdapat *malware* pada jaringan maka proses akan terus berlanjut selama *honeypot dionaea* berjalan. Dari diagram flowchart Gambar 3.2 menunjukan.



Gambar 3.2 Flow Chart deteksi *malware*

3.4 Perancangan sistem

Perangkat lunak yang di bangun dan dilakukan secara sistematis, dengan arti bahwa kemampuan sistem yang dibangun menyerupai bentuk *server*, seolah – olah *server* telah tersisipi oleh *malware*. Pada dasarnya *malware* tersebut masuk kedalam *virtual private server* yang terbentuk oleh *honeypot dionaea*, dan

melakukan pencatatan serangan-serangan *malware* kemudian nantinya didefenisikan pada direktori yang disediakan *honeypot dionaea* merupakan tolak ukur keberhasilan sistem ini. Dengan demikian keberhasilan tolak ukur sistem yang di jalankan untuk melakukan pendeteksian dapat diketahui. . Dan dari hasil *malware* yang tertangkap dalam bentuk kode *binaries*, nantinya akan di dihubungkan ke situs anubis secara random. Sehingga dapat mengetahui jenis aplikasi yang diserang oleh virus *malware*, terindentifikasi dan tercatat secara jelas dalam bentuk file seperti HTML, XML, PDF, Text

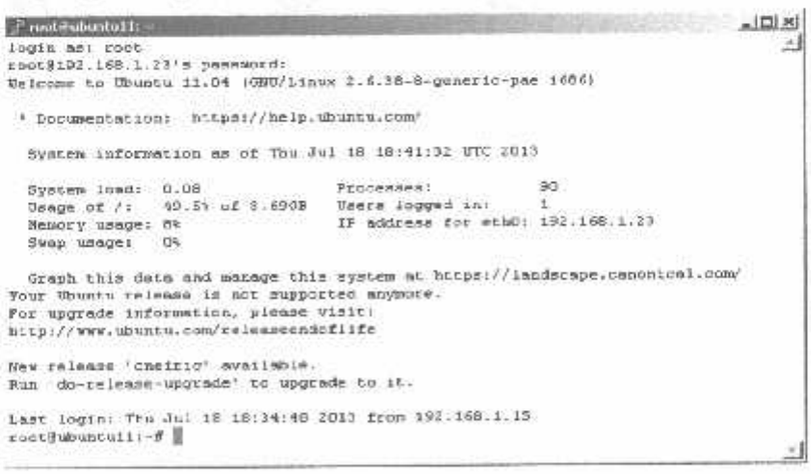
3.5 Implementasi

3.5.1 Instalasi sistem

Sistem operasi yang digunakan adalah *Linux Ubuntu server 11.04* yang di install di dalam *VMware 9*, untuk dijadikan *honeypot dionaea*. Setelah instalasi selesai, *login* sesuai *username* dan *password* yang telah di buat sebelumnya.

1) Masuk *root VPS*

Untuk masuk ke *root VPS* , penulis harus melakukan SSH terlebih dahulu ke IP Publik nya dengan program putty, karena penulis pada waktu login mengendalikan (remot) server. Setelah itu masukan *password* dari *root VPS*. Tampilan layar pada login root ke vps ditunjukan pada gambar 3.3



Gambar 3.3 Masuk ke root VPS

2) *Update* sistem

Update sistem digunakan menginstall *software* yang belum ada di sistem sehingga operasi sistem lebih cocok ketika ada *software- software* baru. ditunjukan pada gambar 3.4.

```
root@ubuntu11:# apt-get update
```

Gambar 3.4 *Update* sistem

3) *Upgrade* sistem

Upgrade sistem adalah menambah atau mempebarui *software* yang sudah ada di sistem ditunjukan pada gambar 3.5

```
root@ubuntu11:# apt-get upgrade
```

Gambar 3.5 *Upgrade* sistem

4) *Install* Paket *Honeypot Dionaea*

Kemudian setelah berhasil masuk *root, install* paket yang dibutuhkan ditunjukan pada gambar 3.6.

```
root@ubuntu11:# aptitude -f install libudns-dev libglib2.0-dev libssl-dev \
libcurl4-openssl-dev libreadline-dev libsqlite3-dev python-dev \
libtool automake autoconf build-essential subversion git-core \
flex bison pkg-config sqlite3 libgc-dev
```

Gambar 3.6 Instalasi paket *honeypot dionaea*

5) Membuat *direktori*

Membuat *direktori* di Ubuntu server 11.04 untuk menambah paket-paket *Honeypot Dionaea.* Setalah itu membuat folder di *"/opt/Dionaea"* dan "Download" , ditunjukan pada gambar 3.7.

```
root@ubuntu11:# mkdir /opt/Dionaea
root@ubuntu11:# mkdir Download
```

Gambar 3.7 Membuat direktori *Dionaea*

6) *Download Liblcfg*

Liblcfg adalah untuk memproses file-file konfigurasi dengan benar dalam skrip shell, masuk ke folder *Download* kemudian *download* dan *install* paket *liblcfg.* ditunjukan pada gambar 3.8.

```
root@ubuntu11:# cd / Download /
root@ubuntu11:~/ Download# git clone git://git.carnivore.it/liblcfg.git liblcfg
root@ubuntu11:~/ Download# cd liblcfg/code/
root@ubuntu11:~/ Download/liblcfg/code# autoreconf -vi
root@ubuntu11:~/ Download/liblcfg/code# ./configure --prefix=/opt/dionaea
root@ubuntu11:~/ Download/liblcfg/code# make install
root@ubuntu11:~/ Download/liblcfg/code# cd ..
root@ubuntu11:~/ Download/liblcfg/code# cd ..
```

Gambar 3.8 *Download Liblcfg*

7) *Download Libemu*

libemu adalah sebuah emulasi x86 dan deteksi shellcode menggunakan *heuristik GetPC*. Hal ini dirancang untuk digunakan dalam intrusi / pencegahan deteksi jaringan dan *honeypot* dionaea. Kemudian *download* dan *install* paket yang *libemu,* ditunjukan pada gambar 3.9.

```
root@ubuntu11:# cd / Download /
root@ubuntu11:~/ Download# git clone git://git.carnivore.it/libemu.git libemu
root@ubuntu11:~/ Download# cd libemu
root@ubuntu11:~/ Download/libemu# autoreconf -vi
root@ubuntu11:~/ Download/libemu# ./configure –prefix=/opt/dionaea
root@ubuntu11:~/ Download/libemu# make install
root@ubuntu11:~/ Download/libemu# cd ..
```

Gambar 3.9 *Download Libemu*

8) *Download Libnl*

Libnl adalah *libraries* yang menyediakan API (*Application Programing Interface*) untuk netlink protokol berbasis Linux kernel interface. Netlink adalah mekanisme IPC (*Integrated Protocol Converter*) primarly antara kernel dan proses ruang pengguna. Hal ini dirancang untuk menjadi pengganti yang lebih fleksibel untuk IOCTL (*IO-ConTroL*) untuk memberikan terutama jaringan konfigurasi kernel yang terkait dan antarmuka pemantauan. kemudian *download* dan *install* paket yang *Libnl* ditunjukan pada gambar 3.10

```
root@ubuntu11:# cd / Download /
root@ubuntu11:~/ Download# git clone git://git.infradead.org/users/tgr/libnl.git libnl
root@ubuntu11:~/ Download# cd libnl
root@ubuntu11:~/ Download/libnl# autoreconf -vi
root@ubuntu11:~/ Download/libnl# ./configure --prefix=/opt/dionaea
root@ubuntu11:~/ Download/libnl# make install
root@ubuntu11:~/ Download/libnl# cd ..
```

Gambar 3.10 *Download Libemu*

12) *Download Cython*

Cython adalah bahasa pemrograman berbasis *Python*, dengan sintaks tambahan memungkinkan untuk deklarasi tipe statis opsional. Hal ini bertujuan untuk menjadi superset dari *Python* bahasa yang memberikan tingkat tinggi, *object-oriented*, fungsional, dan pemrograman dinamis. Kode sumber akan diterjemahkan menjadi dioptimalkan C / C + + kode dan dikompilasi sebagai modul ekstensi *Python*. Hal ini memungkinkan untuk kedua eksekusi program sangat cepat dan integrasi yang erat dengan perpustakaan C eksternal, sambil menjaga produktivitas programmer tinggi yang bahasa Python terkenal., kemudian *download* dan *install* paket yang *Cython* ditunjukan pada gambar 3.14.

```
root@ubuntu11:# cd / Download /
root@ubuntu11:~ /Download# wget http://cython.org/release/Cython-0.15.1.tar.gz
root@ubuntu11:~ /Download# tar xzvf Cython-0.15.1.tar.gz
root@ubuntu11:~ /Download# cd Cython-0.15.1/
root@ubuntu11:~ /Download/Cython-0.15.1# /opt/dionaea/bin/python3 setup.py install
root@ubuntu11:~ /Download/Cython-0.15.1# cd ..
```

Gambar 3.14 *Download Cython*

13) *Download Udns*

UDNS adalah rintisan DNS menyelesaikan perpustakaan dengan kemampuan untuk melakukan keduanya sinkron dan ansinkron query DNS, kemudian *download* dan *install* paket yang *Udns* ditunjukan pada gambar 3.15.

```
root@ubuntu11:~ /Download# wget http://www.corpit.ru/mjt/udns/old/udns_0.0.9.tar.gz
root@ubuntu11:~ /Download# tar xfz udns_0.0.9.tar.gz
root@ubuntu11:~ /Download# cd udns-0.0.9/
root@ubuntu11:~ /Download/udns-0.0.9# ./configure
root@ubuntu11:~ /Download/udns-0.0.9# make shared
root@ubuntu11:~ /Download/udns-0.0.9# cd ..
```

Gambar 3.15 *Download Udns*

14) Salin folder *Udns*

Menggandakan folder *libudns* agar file yang default masih ada, ditunjukan pada gambar 3.16.

```
root@ubuntu11:~ /Download/udns-0.0.9# cp udns.h /opt/dionaea/include/
root@ubuntu11:~ /Download/udns-0.0.9# cp *.so* /opt/dionaea/lib/
root@ubuntu11:~ /opt/dionaea/lib# ln -s libudns.so.0 libudns.so
root@ubuntu11:~ /opt/dionaea/lib# cd -
root@ubuntu11:~ /Download/udns-0.0.9# cd ..
```

Gambar 3.16 salin folder *udns*

15) *Download Libpcap*

Libpcap menyediakan portabel kerangka kerja untuk memonitor jaringan tingkat rendah. aplikasi termasuk koleksi jaringan statistik, pemantauan keamanan, debugging jaringan, karena hampir setiap vendor sistem menyediakan antarmuka yang berbeda untuk capture paket, dan mengembangkan beberapa alat bantu yang membutuhkan fungsi membuat ini API sistem independen untuk memudahkan dalam port dan mengurangi kebutuhan untuk beberapa bergantung pada sistem paket modul capture dalam setiap aplikasi. Kemudian *download* dan *install* paket yang *Libpcap* ditunjukan pada gambar 3.17.

```
root@ubuntu11:~ /Download# wget http://www.tcpdump.org/release/libpcap-1.2.1.tar.gz
root@ubuntu11:~ /Download# tar xzvf libpcap-1.2.1.tar.gz
root@ubuntu11:~ /Download# cd libpcap-1.2.1/
root@ubuntu11:~ /Download/ libpcap-1.2.1# ./configure --prefix=/opt/dionaea
root@ubuntu11:~ /Download/ libpcap-1.2.1# make
root@ubuntu11:~ /Download/ libpcap-1.2.1# make install
root@ubuntu11:~ /Download/ libpcap-1.2.1# cd ..
```

Gambar 3.17 *Download Libpcap*

16) *Download Dionaea*

Dionaea adalah untuk menjebak kerentanan memanfaatkan malware terpapar oleh layanan sebuah jaringan, tujuan utama adalah mendapatkan salinan dari malware. kemudian *download* dan *mengcompile* paket yang *Dionaea* ditunjukan pada gambar 3.18

```
root@ubuntu11:~ /Download# git clone git://git.carnivore.it/dionaea.git dionaea
                        root@ubuntu11:~ /Download# cd dionaea/
root@ubuntu11:~ /Download/dionaea# autoreconf -vi
root@ubuntu11:~ /Download/dionaea# ./configure --with-lcfg-include=/opt/dionaea/include/
\
   --with-lcfg-lib=/opt/dionaea/lib/ \
   --with-python=/opt/dionaea/bin/python3.2 \
   --with-cython-dir=/opt/dionaea/bin \
   --with-udns-include=/opt/dionaea/include/ \
   --with-udns-lib=/opt/dionaea/lib/ \
   --with-emu-include=/opt/dionaea/include/ \
   --with-emu-lib=/opt/dionaea/lib/ \
   --with-gc-include=/usr/include/gc \
   --with-ev-include=/opt/dionaea/include \
   --with-ev-lib=/opt/dionaea/lib \
   --with-nl-include=/opt/dionaea/include \
   --with-nl-lib=/opt/dionaea/lib/ \
   --with-curl-config=/usr/bin/ \
```

```
    --with-pcap-include=/opt/dionaea/include \
    --with-pcap-lib=/opt/dionaea/lib/
root@ubuntu11:~ /Download/dionaea# make
root@ubuntu11:~ /Download/dionaea# sudo make install
root@ubuntu11:~ /Download/dionaea# cd ..
```

Gambar 3.18 *Download Dionaea* dan *mengcompile*

3.5.2 Instalasi Django 1.4

1) Install *Djang*o

Django adalah kerangka Web *Python* tingkat tinggi yang mendorong perkembangan pesat dan bersih, desain pragmatis (hasil yang bermanfaat secara praktis). Dikembangkan oleh operasi online-berita yang bergerak cepat, *Django* dirancang untuk menangani dua tantangan: tenggat waktu intensif ruang berita dan persyaratan ketat dari pengembang Web berpengalaman yang menulisnya. Ini memungkinkan Anda membangun berkinerja tinggi, aplikasi Web elegan cepat. Cara menginstal *Django* ditunjukan pada gambar 3.19.

```
root@ubuntu11:~ /opt# apt-get install pip
root@ubuntu11:~ /opt#pip install Django
```

Gambar 3.19 Install django

2) Install *Pygeoip*

GeoIP adalah library C yang memungkinkan pengguna untuk menemukan informasi geografis dan jaringan dari alamat IP. Untuk menggunakan library ini, Anda dapat men-download gratis kami GeoLite Negara atau Kota database. Cara menginstal *Pygeoip* ditunjukan pada gambar 3.20.

```
root@ubuntu11:~ /opt# pip install pygeoip
```

Gambar 3.20 Install *Pygeoip*

3) Install *django-pagination*

Cara menginstal *django-pagination* ditunjukan pada gambar 3.21.

```
root@ubuntu11:~ /opt# pip install django-pagination
```

Gambar 3.21 Instal *django-pagination*

4) Install *django-table2*

Cara menginstal *django-table2* ditunjukan pada gambar 3.22.

```
root@ubuntu11:~ /opt# pip install django-tables2
```

Gambar 3.22 Install *django-table2*

5) Install *django-compressor*

Cara menginstal *django-compressor* ditunjukan pada gambar 3.23.

```
root@ubuntu11:~ /opt# pip install django-compressor
```

Gambar 3.23 Install *django-compressor*

6) Install *django-htmlmin*

Cara menginstal *django-htmlmin* ditunjukan pada gambar 3.24.

```
root@ubuntu11:~ /opt# pip install django-htmlmin
```

Gambar 3.24 Install *django-htmlmin*

7) Download *django- table2-simplefilter*

Cara menginstal *django-htmlmin* ditunjukan pada gambar 3.25

```
root@ubuntu11:~ /opt# git clone https://github.com/benjiec/django-tables2-
simplefilter
root@ubuntu11:~ /opt# python setup.py install
```

Gambar 3.25 Download *django- table2-simplefilter*

8) Download *nodejs*

Sebuah website yang mengembangkan Node.js mendeskripsikan kalau skrip mereka secara esensial akan mampu menangani event input output untuk javascript, dengan kata lain, toolkit ini dapat memungkinkan para developer javascripts untuk membuat event-driven servers dalam *JavaScript*. Cara menginstal *nodejs* ditunjukan pada gambar 3.26.

```
root@ubuntu11:~ /opt# wget http://nodejs.org/dist/v0.8.16/node-v0.8.16.tar.gz
root@ubuntu11:~ /opt# tar xzvf node-v0.8.16.tar.gz
root@ubuntu11:~ /opt# cd node-v0.8.16
root@ubuntu11:~ /opt/ node-v0.8.16# make
root@ubuntu11:~ /opt/ node-v0.8.16# make install
root@ubuntu11:~ /opt/ node-v0.8.16# npm install -g less
root@ubuntu11:~ /opt/ node-v0.8.16# apt-get install python-netaddr
```

Gambar 3.26 Download *nodejs*

9) Download *GeoIP*

Cara menginstal *GeoIP* ditunjukan pada gambar 3.27.

```
root@ubuntu11:~ /opt# wget
http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
```

Gambar 3.27 Download *GeoIP*

10) Download *GeoLiteCity*

Cara menginstal *GeoLiteCity* ditunjukan pada gambar 3.28

```
root@ubuntu11:~ /opt# wget
http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz
```

Gambar 3.28 Download *GeoIP*

11) *Decompress GeoIP*

Cara *Decompress GeoIP* ditunjukan pada gambar 3.29.

```
root@ubuntu11:~ /opt# gunzip GeoIP.dat.gz
```

Gambar 3.29 *Decompress GeoIP*

12) *Decompress GeoLiteCity*

Cara *Decompress GeoLiteCity* ditunjukan pada gambar 3.30.

```
root@ubuntu11:~ /opt# gunzip GeoLiteCity.dat.gz
```

Gambar 3.30 *Decompress GeoLiteCity*

13) Memindahkan *GeoIP* ke direktori *"DionaeaFR/DionaeaFR/"*

Cara memindahkan *GeoIP* ditunjukan pada gambar 3.31.

```
root@ubuntu11:~ /opt# mv GeoIP.dat DionaeaFR/DionaeaFR/static
```

Gambar 3.31 Memindahkan *GeoLiteCity*

14) Memindahkan *GeoLiteCity* ke direktori *"DionaeaFR/DionaeaFR/"*

Cara memindahkan *GeoLiteCity* ditunjukan pada gambar 3.32.

```
root@ubuntu11:~ /opt# mv GeoLiteCity.dat DionaeaFR/DionaeaFR/static
```

Gambar 3.32 Memindahkan *GeoLiteCity*

15) Untuk menjalankan server *DionaeaFR*

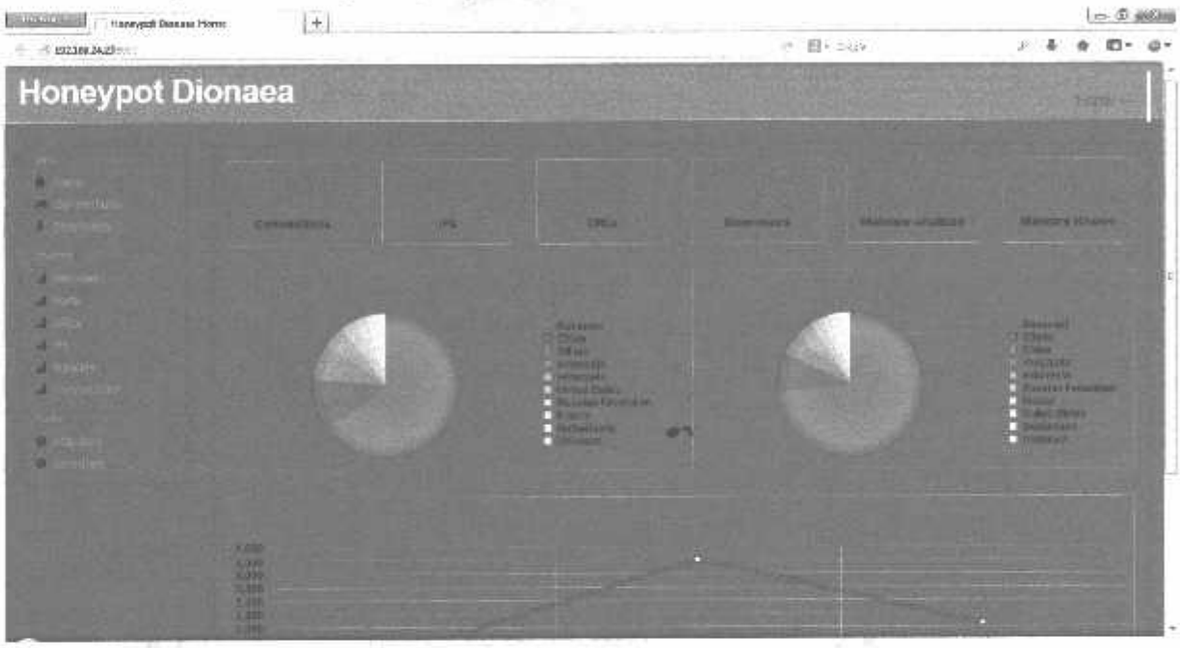
Cara memindahkan *GeoLiteCity* ditunjukan pada gambar 3.33

```
root@ubuntu11:~ /opt# cd DionaeaFR
root@ubuntu11:~ /opt/DionaeaFR#python manage.py runserver 0.0.0.0:8090
```

Gambar 3.33 Memindahkan *GeoLiteCity*

16) Tampilan *Django Honeypot Dionaea (DionaeaFR)*

Untuk menampilkan beberapa IP yang menyerang ditunjukan pada gambar 3.34.



Gambar 3.34 Tampilan dari *Honeypot Dionaea (DionaeaFR)*

BAB IV
IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Kebutuhan Sistem

Dalam melakukan implementasi dan pengujian sistem dibutuhkan suatu perangkat keras dan beberapa perangkat lunak agar sistem bisa berjalan dengan baik.

4.2 Spesifikasi sistem

Dalam membangun suatu *honeypot dionaea* dibutuhkan perangakat keras dan perangkat lunak yang memenuhi spesifikasi yang dibutuhkan.

1. Hardware

a. Notebook M505
b. Prosesor Core2 Duo
c. RAM 4GB
d. Hardisk 250 GB
e. Modem router TPLink

Sedangkan untuk perangkat lunak yang dibutuhkan dalam membangun *honeypot dionaea* diperlukan *software-software*

1. *Software*

a. Sistem operasi Linux Ubuntu server 11.04
b. Putty
c. VMware 9
d. Udns
e. Libcap
f. Dionaea
g. Libnl
h. Cython
i. Python
j. Sqlite
k. Libev
l. Liblcfg

m. Libemu

n. Nmap

o. Django

4.3 Pengujian

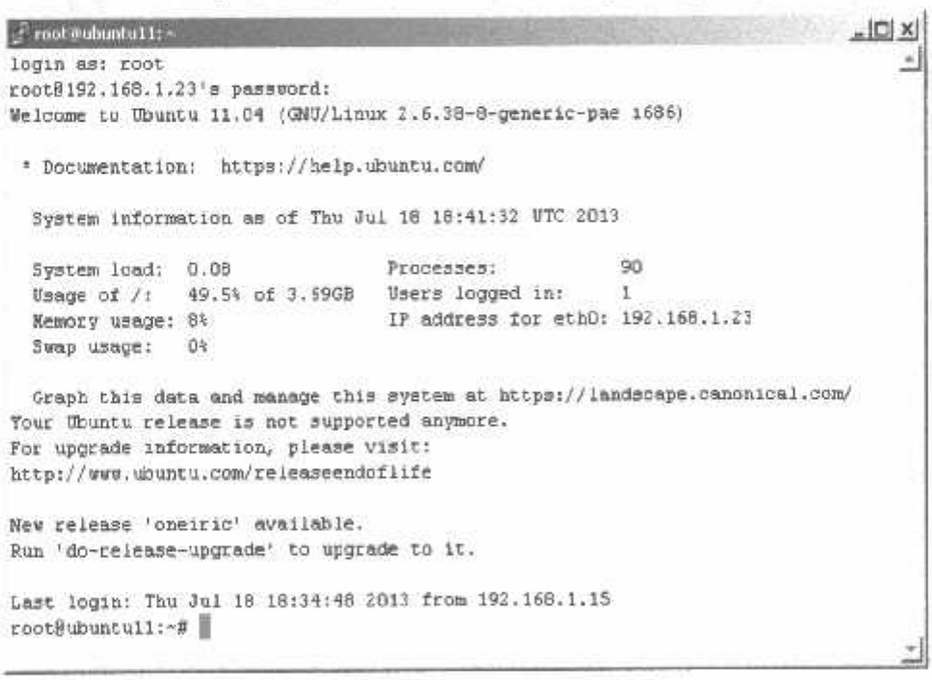
4.3.1 Prosedur pengujian

Pengujian dilakukan dari selasa 19 mei 2013 pukul 22.00 sampai 23 mei 2013 pukul 23.00. Pada hari sabtu 13 juli 2013 pada pukul 22.51 sampai 14 juli 2013 pada pukul 22.30 di jaringan internet dengan menggunakan IP publik. Pengujian ini dilakukan dengan tujuan mengimplementasikan *honeypot dionaea* dalam menangkap serangan *malware.*

4.3.2 Pengujian Sistem

Langkah 1 Pengujian

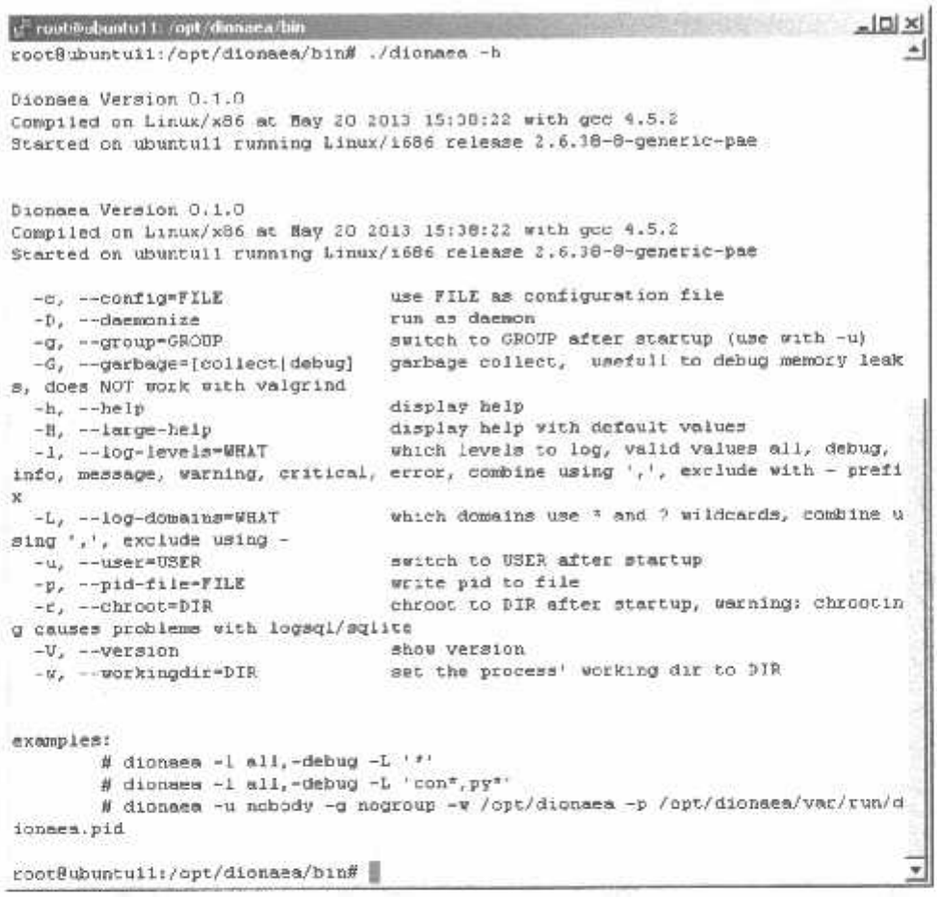
Masuk ke *root* IP public nya dahulu dengan ditunjukan pada gambar 4.1.



Gambar 4.1 Masuk kedalam server

Langkah 2 pengujian

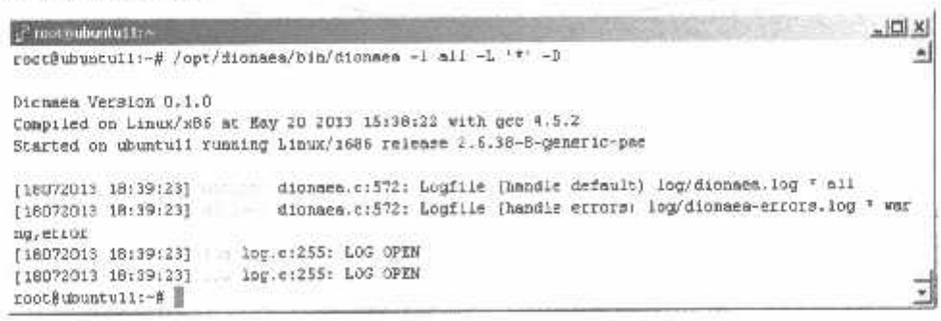
Masuk ke direktori "/opt/dionaea/bin" dengan perintah berikut ditunjukan pada gambar 4.2.



Gambar 4.2 Perintah pada *dionaea*

Langkah 3 pengujian

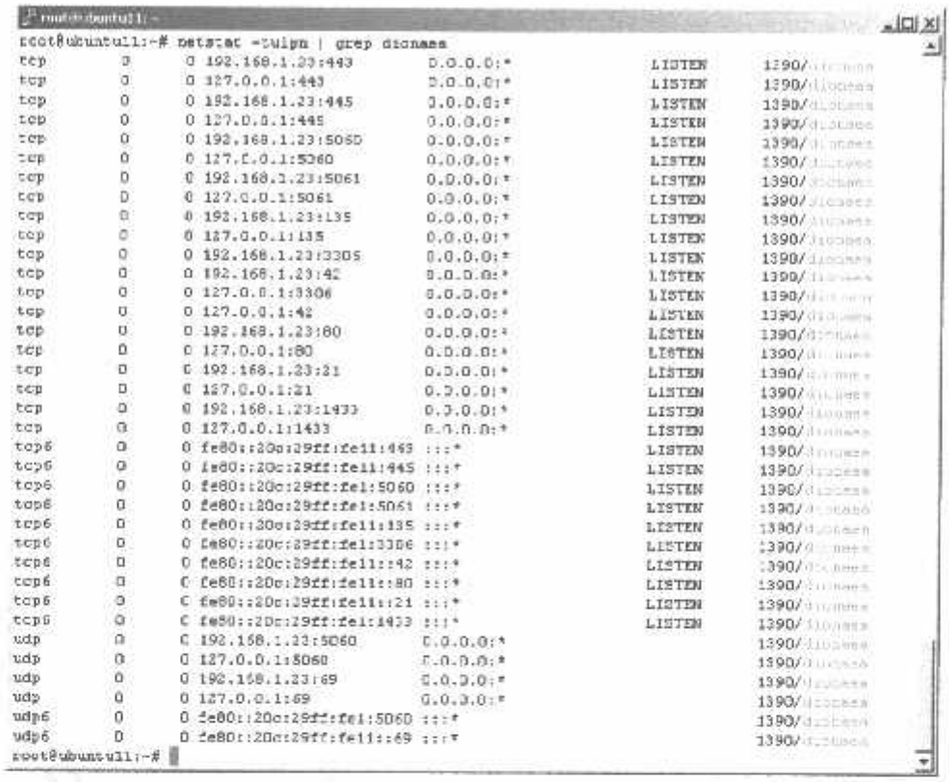
Lalu menjalankan *honeypot dionaea* dengan perintah berikut pada ditunjukan pada gambar 4.3



Gambar 4.3 Menjalankan *Dionaea*

Langkah 4 pengujian

Lalu untuk melihat port – port dari Dionaea yang sudah terbangun, ketikkan perintah ditunjukan pada gambar 4.4



Gambar 4.4 Melihat port yang dijalan pada *dionaea*

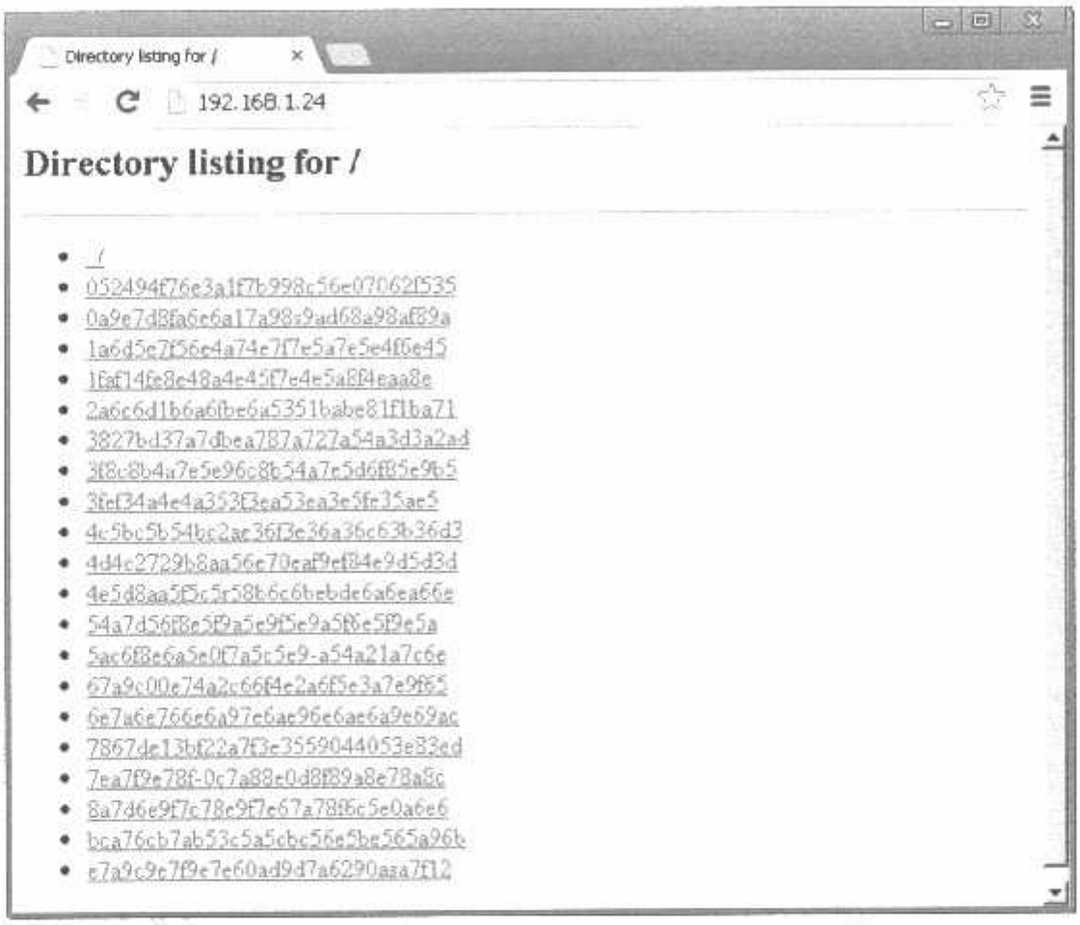
Langkah 5 pengujian

Untuk lebih memastikan bahwa *Honeypot* sudah benar – benar terbangun, maka uji coba menggunakan Nmap ditunjukan pada gambar 4.5.

Gambar 4.5 Pengujian dengan *Nmap*

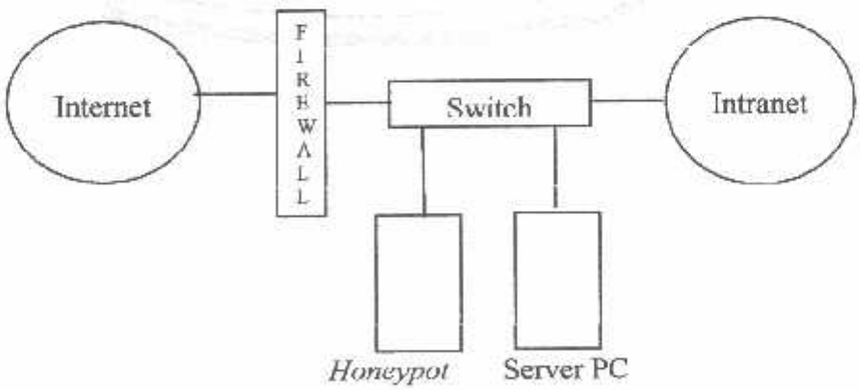
Langkah 7

Melihat hasil dari mengubah *setting* dari file "*dionaea.conf*" ditunjukan pada gambar 4.8



Gambar 4.8 Malware dilihat di *browser*

4.3.3 Diagram Sistem *Honeypot Dionaea*



Gambar 4.9 Sistem *honeypot dionaea*

Gambar 4.9 menunjukan sistem *Honeypot* yang digunakan di jaringan *internet*. Ada firewall untuk menangkap lalu lintas masuk dan keluar yang juga menyediakan jaringan *Address Translation* atau NAT. Server PC akan mengumpulkan informasi untuk masuk lalu lintas dan perintah yang dieksekusi oleh hacker yang masuk ke dalam jaringan. PC yang berisi *honeypot* akan memiliki perangkat lunak *honeypot* untuk mengumpulkan semua informasi yang diperlukan berkaitan dengan *hacker*. *Honeypot* diinstal dengan VMWARE Workstation yang maka akan dapat menjalankan beberapa sistem operasi seperti Windows 2000, Linux dan Unix. Ini diagram jaringan khas dari *Honeynet* akan sangat berguna jika digunakan dalam jaringan internet

4.3.4 Hasil Analisis *Malware*

Langkah 1

Membuka *browser* dengan ke situs http://anubis.iseclab.org/ untuk mengetahui diskripsi dari *malware* yang tertangkap di *honeypot dionaea* ditunjukan pada gambar 4.10

Gambar 4.10 Membuka situs *anubis*

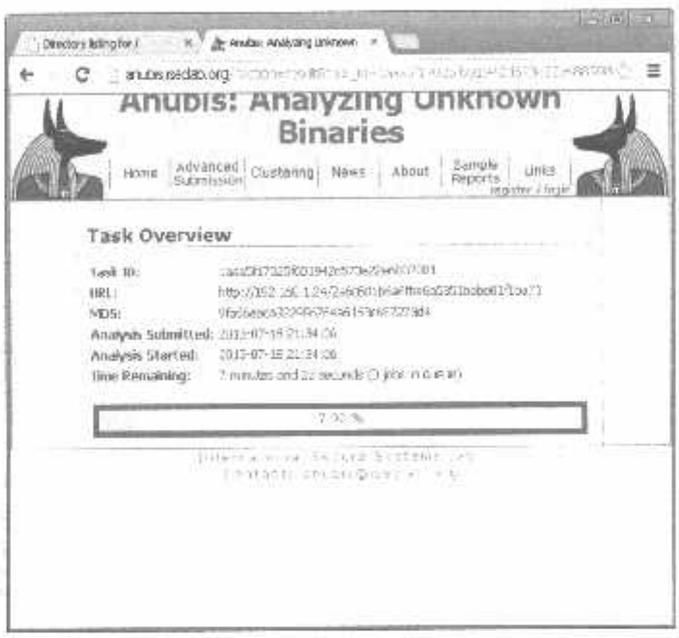
Langkah 2

Buka *browser* dengan alamat IP Address Dioanaea IP Local (*Privat NAT*) 192.168.1.24 ditunjukan pada gambar 4.11.

Gambar 4.11 Melihat file *malware* di *browser*

Langkah 3

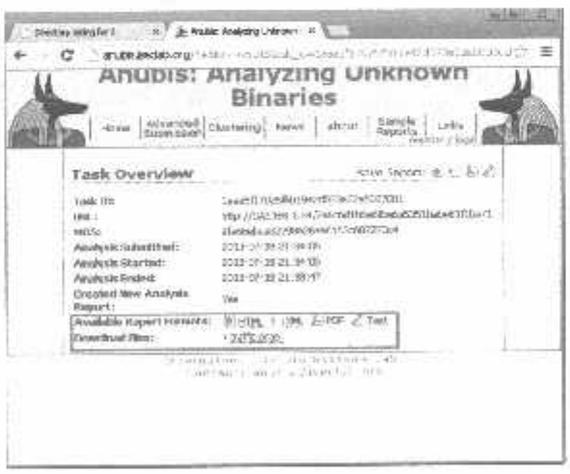
Membuka situs *anubis* dan pilih untuk URL (Uniform Resource Locator)Dan pilih salah satu malware yang berada di browser IP address *dionaea*.Masukan kode yang ada pada "*Get a priority boost*" lalu *submit for analysis* ditunjukan pada gambar 4.12.



Gambar 4.12 Melihat file *malware* di *browser*

Langkah 4

Setelah selesai proses analisa di situs *anubis* ada pilihan untuk menampilkan dalam bentuk file *html, xml, pdf, text.* ditunjukan pada gambar 4.13.



Gambar 4.13 Hasil file dari site *anubis*

Langkah 5

Hasil dari diskripsi *malware* dari situs *anubis* dengan format file *html* ditunjukan pada gambar 4.14.

Gambar 4.14 Hasil analis *malware* versi html

Langkah 6

Agar dapat menganalisa *malware* dengan mudah penulis menambah program web ditunjukan pada gambar 4.15

Gambar 4.15 Program bantuan analisis *malware*

4.4 Tabel Pengujian

Berikut tabel pengujian program yang telah menerima 25 serangan *malware* ke server dan 2 gagal tertangkap *honeypot dionaea.*

Tabel 4.1 Tertangkapnya *malware*

Attacker	Malware Tertangkap
1	0a9e7d8fa6e6a17a98s9ad68a98af89a
2	1a6d5e7f56e4a74e7f7e5a7e5e4f6e45
3	1faf14fe8e48a4e45f7e4e5a8f4eaa8e
4	GAGAL
5	2a6c6d1b6a6fbe6a5351babe81f1ba71
6	3f8c8b4a7e5e96c8b54a7e5d6f85e9b5
7	3fef34a4e4a353f3ea53ea3e5fe35ae5
8	4c5bc5b54bc2ae36f3e36a36c63b36d3
9	4d4c2729b8aa56e70eaf9ef84e9d5d3d
10	4e5d8aa5f5c5r58b6c6bebde6a6ea66e
11	5ac6f8e6a5e0f7a5c5e9-a54a21a7c6e
12	6e7a6e766e6a97e6ae96e6ae6a9e69ac
13	7ea7f9e78f-0c7a88e0d8f89a8e78a8c
14	GAGAL
15	8a7d6e9f7c78e9f7e67a78f6c5e0a6e6
16	5eca5bc7b01ae1b4feb08c5d304d1fe4
17	54a7d56f8e5f9a5e9f5e9a5f6e5f9e5a
18	67a9c00e74a2c66f4e2a6f5e3a7e9f65
19	3827bd37a7dbea787a727a54a3d3a2ad
20	7867de13bf22a7f3e3559044053e83ed
21	052494f76e3a1f7b998c56e07062f535
22	bca76cb7ab53c5a5cbc56e5be565a96b
23	d4315bc7001ae1247eb08c5d304d1bd4
24	e7a9c9e7f9e7e60ad9d7a6290asa7f12
25	4aca5bcfab1a51b4fed0fc5d3add1bd4

hasil dari serangan *Malware* pada tabel 4.4.1 dijelaskan dengan persentasi 92% malware dapat di tangkap oleh *honeypot* dan 8% tidak dapat di tangkap.

Dari perhitungan $\frac{23}{25} \times 100\ \% = 92\ \%$ keberhasilan

dan kegagalan $100\ \% - 92\ \% = 8\ \%$

4.5 Hasil *analisis malware*

Dari mengambil bebarapa contoh malware yang tertangkap oleh *honeypot dioanaea*

Tabel 4.2 Hasil *Analisis malware*

Malware	Hasil Analisis	Diskripsi
052494f76e3a1f7b998c56e07062f535	Modifikasi aplikasi	dapat dijalankan tetapi apliaksi tidak berjalan dengan normal
	menjalankan aktifitas registrasi	dapat dijalakan dan mengubah nilai entri registry
	merubah pengaturan kemaman IE	mempengaruhi keamanan ketika membuka web()
	mengubah nilai memory	dapat dijalankan dengan proses lain
	mengupdate email	mencari log aktivitas jaringan
	menduplikasi aplikasi dan perusakan	dapat dijalakan dan merusak pada system 32 pada windows
0a9e7d8fa6e6a17a98s9ad68a98af89a	Modifikasi aplikasi	dapat dijalankan tetapi aplikasi tidak berjalan dengan normal
	menjalankan aktifitas registrasi	dapat dijalankan dan mengubah nilai entri registry
	merubah pengaturan keamanan IE	mempengaruhi keamanan ketika membuka web()
	mengubah nilai memory	dapat dijalankan dengan proses lain
e7a9c9e7f9e7e60ad9d7a6290asa7f12	Modifikasi aplikasi	dapat dijalankan tatapi aplikasi tidak berjalan dengan normal
	menjalankan aktifitas registrasi	dapat dijalakan dan mengubah nilai entri registry
	menduplikasi aplikasi	merubah aplikasi explorer di windows untuk

		mendapatkan log aktifitas
	mengubah nilai memory	dapat dijalankan dengan proses lain

Dari contoh analisa *malware* pada tabel 4.2 yang didapatkan dari hasil *honeypot dionaea* dalam menangkap *malware*, adalah hasil *kode binaries* yang telah link kan dari alamat *IP address* dari *honeypot dionaea* menggunakan situs *anubis.iseclab.org*. Yang berfungsi dari situs *anubis.iseclab.org* tersebut adalah memberikan layanan untuk analisa *malware*. Karena *honeypot dionaea* itu sendiri jenisnya *low interaction honeypot* yang bersifat koneksi satu arah, maka hanya satu sisi. Yaitu dari sisi *honeypot* yang mendeteksi dan mencatat koneksi yang terjadi tanpa memberikan balasan kepada koneksi tersebut.

BAB V
PENUTUP

5.1 Kesimpulan

1. Sistem *honeypot dionaea* dapat mendeteksi *Malware*. Sistem *honeypot dionaea* dapat merekam serangan dari attacker PC .*Honepot Dionaea* di letakan jaringan *internet* dengan menggunakan IP publik.

2. Sistem *honeypot dionaea* berdasarkan tabel 4.1 memberikan hasil sebesar 92 % pada tingkat keberhasilan sistem, 8 % gagal pengujian dalam pendeteksian *malware* dari sebuah attacker PC.

5.2 Saran

Berdasarkan kesimpulan dari sistem *honeypot dionaea* maka penulis ingin menyampaikan saran yaitu, diharapkan deteksi dan analisis *malware* ini dapat dikembangkan secara optimal dan dapat menampilkan notifikasi disetiap adanya serangan malware, *honeypot dionaea* dapat digunakan untuk mengantisipasi serangan *Malware* terhadap jaringan komputer.

DAFTAR PUSTAKA

[1] Kadir ,Abdul,2005,*Python*,Andi,Yogyakarta.

[2] Mansfield, Niall,2004,*Practical TCP/IP Jilid 1 dan 2*,Andi,Yogyakarta.

[3] Michael Davis, Sean Bodmer, Aaron LeMasters,2009, *Hacking Exposed Malware and Rootkits*,New York Chicago San Francisco,Mc Graw Hill.

[4] Purbo,Onno W,D Sembiring,Akhmad,2004,*Apache Web Server*.Elex Media Koputindo,Jakarta

[5] Syafii,M,2004,*Konfigurasi Server Linux Dan Webmin*,Andi,Yogyakarta.

[6] Arief M, 2012, *Implementasi Honeypot Dengan Menggunakan Dionaea Di Jaringan Hotspot FIZZ*,Bandung,Politeknik Telkom (1-8)

[7] Arif ,Yulianto Fazmah, *Honeypot Sebagai Alat Bantu Pendeteksian Serangan pada Jaringan Komputer*, (budi.insan.co.id/courses/el7010/2003/report-arif.pdf (4-5). di Akses Online 29 Juli 2013)

[8] Wafa,Rendra. *Pengertian NAT dan Tipe - Tipe NAT*, (http://www.jejaring.web.id/pengertian-nat-dan-tipe-tipe-nat. diakses Online pada 10 Juni 2013)

[9] Anonymous.*Pengertian NMap*, (http://www.bunganajwa.com/2010/03/pengertian-nmap.html#.Ufqug6yr9KE. di Akses Online 20 Juli 2013)

[10] Anonymous, *Contoh Awal Penggunaan Putty untuk Mengakses VPS Melalui Port SSH*,(http://www.panda-undetected.org/2013/04/contoh-awal-penggunaan-putty-untuk.html. Di Akses Online 16 Juli 2013)

[11] Anonymous, *dionaea catches bugs*, (http://dionaea.carnivore.it/. di Akses Online 16 Juli 2013)

LAMPIRAN

PROGRAM STUDI TEKNIK INFORMATIKA S-1
INSTITUT TEKNOLOGI NASIONAL MALANG
Jln. Raya Karanglo, Km2
MALANG

FORMULIR BIMBINGAN SKRIPSI

Nama : Setyo Wardoyo
NIM : 0918124
MasaBimbingan : 11 Mei 2013 s/d 11 November 2013
Judul Skripsi : PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET

NO	TANGGAL	URAIAN	PARAF PEMBIMBING
1.	10 Juli 2013	Bab 1	
2.	11 Juli 2013	Bab 2	
3.	15 Juli 2013	Bab 3 dan Penulisan	
4.	16 Juli 2013	Bab 3 ACC	
5.	20 Juli 2013	Revisi Bab 4	
6.	23 Juli 2013	ACC dan Bab 4	
7.	23 Juli 2013	ACC Bab 5 Dan Buat makalah seminar hasil	
8.	24 Juli 2013	ACC makalah seminar hasil	

Malang,23 Agustus 2013
DosenPembimbing I

Joseph Dedy Irawan, ST, MT
NIP.19740416 200501 1 002

PROGRAM STUDI TEKNIK INFORMATIKA S-1
INSTITUT TEKNOLOGI NASIONAL MALANG
Jln. Raya Karanglo, Km2
MALANG

FORMULIR BIMBINGAN SKRIPSI

Nama : Setyo Wardoyo
NIM : 0918124
MasaBimbingan : 11 Mei 2013 $^{s}/_{d}$ 11 November 2013
Judul Skripsi : PERANCANGAN APLIKASI ANALISIS DETEKSI KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT DIONAEA* PADA JARINGAN INTERNET

NO	TANGGAL	URAIAN	PARAF PEMBIMBING
1.	11 Juli 2013	Bab 1dan 2	
2.	15 Juli 2013	Bab 3 dan Penulisan	
3.	16 Juli 2013	Bab 3 ACC	
4.	20 Juli 2013	Revisi Bab 4	
5.	23 Juli 2013	ACC dan Bab 4	
6.	23 Juli 2013	ACC Bab 5 Dan Buat makalah seminar hasil	
7.	24 Juli 2013	ACC makalah seminar hasil	

Malang, 23 Agustus 2013
DosenPembimbing II

Sonny Prasetio, ST, MT
NIP.P. 1031000433

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Nomor : ITN-78/T.INF/TA/2013 11 Mei 2013
Lampiran :
Perihal : Bimbingan Skripsi

Kepada : Yth. Bpk/Ibu Sonny Prasetio, ST, MT.
Dosen Pembimbing Program Studi Teknik Informatika S1
Institut Teknologi Nasional
M a l a n g

Dengan hormat
Sesuai dengan permohonan dan persetujuan dalam Proposal Skripsi untuk mahasiswa :

Nama	:	SETYO WARDOYO
Nim	:	0918124
Prodi	:	Teknik Informatika S1
Fakultas	:	Teknologi Industri

Maka dengan ini pembimbingan tersebut kami serahkan sepenuhnya kepada Bpk/Ibu selama masa waktu 6 (enam) bulan, terhitung mulai tanggal ;

11 Mei 2013 – 11 Nopember 2013

Sebagai satu syarat untuk menempuh Ujian Sarjana Teknik, Program Studi Teknik Informatika S1.
Demikian agar maklum dan atas perhatian serta bantuannya kami sampaikan terima kasih.

Mengetahui
Program Studi Teknik Informatika S1
K e t u a,

Joseph Dedy Irawan, ST, MT
NIP : 197404162005021002

Form S-4a

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Nomor : ITN-78/T.INF/TA/2013 11 Mei 2013
Lampiran : -
Perihal : Bimbingan Skripsi

Kepada : Yth. Bpk/Ibu Joseph Dedy Irawan, ST, MT
Dosen Pembimbing Program Studi Teknik Informatika S1
Institut Teknologi Nasional
M a l a n g

Dengan hormat
Sesuai dengan permohonan dan persetujuan dalam Proposal Skripsi untuk mahasiswa :

Nama	:	SETYO WARDOYO
Nim	:	0918124
Prodi	:	Teknik Informatika S1
Fakultas	:	Teknologi Industri

Maka dengan ini pembimbingan tersebut kami serahkan sepenuhnya kepada Bpk/Ibu selama masa waktu 6 (enam) bulan, terhitung mulai tanggal ;

11 Mei 2013 – 11 Nopember 2013

Sebagai satu syarat untuk menempuh Ujian Sarjana Teknik, Program Studi Teknik Informatika S1.
Demikian agar maklum dan atas perhatian serta bantuannya kami sampaikan terima kasih.

Mengetahui
Program Studi Teknik Informatika S1
K e t u a,

Joseph Dedy Irawan, ST, MT
NIP : 197404162005021002

Form S-4a

INSTITUT TEKNOLOGI NASIONAL MALANG
Fakultas Teknologi Industri
Program Studi Teknik Informatika S1

FORMULIR PERBAIKAN UJIAN SKRIPSI

Dalam pelaksanaan Ujian Skripsi Jenjang Strata 1 Jurusan Teknik Informatika, maka perlu adanya perbaikan untuk mahasiswa :

Nama : Heru Wardoyo
NIM : 09.17.124
Perbaikan Meliputi :

1) Hal 20 s/d 21 jadikan satu terlalu banyak kosong
2) Daftar Pustaka → Perbaiki
Daftar Pustaka ini harus ADA yg dari buku, ~~atau~~ jurnal, atau ebook
3) Perbaiki Referensi
semua di bab 1 s/d 2, harus ada dasar referensi di daftar pustaka
4) Perbaiki no gambar. Ada double gambar 3.23 di hal 34 s/d 35
5) Hal 43 s/d 44 Ada double langkah 6
6) Batasan Masalah No 5
7) Demo jika ada kerangan, muncul notifikasi

Malang, 15 Agustus 2013

(ALDAMIND)

INSTITUT TEKNOLOGI NASIONAL MALANG
Fakultas Teknologi Industri
Program Studi Teknik Informatika S1

FORMULIR PERBAIKAN UJIAN SKRIPSI

Dalam pelaksanaan Ujian Skripsi Jenjang Strata 1 Jurusan Teknik Informatika, maka perlu adanya perbaikan untuk mahasiswa :

Nama : Seivo Wanoleya
NIM : 09.10.124
Perbaikan Meliputi :

1. Perbaiki format penulisan
2. Perbaiki flowchart Gambar 3.2 (hal. 23)
3. Perbaiki batasan masalah.
4. Tambah kesimpulan dan saran.
5. Menambah notifikasi di admin jika ada serangan Malware.

Malang, 5 Januari 2013

(Yusep Rosmansyah)

Source code (index.html)

```
<html>
  <head><title>Analisi deteksi Malware</title>
  <link rel="stylesheet" href="mod2.php_files/style.css" type="text/css">
  </head>
<frameset rows=20%,* framespacing="0" border="1" frameborder="0">
  <frame name=atas src=atas.html noresize>
<frameset cols=15%,* framespacing="0" border="1" frameborder="0">
  <frame name=kiri src=kiri.html  noresize>
  <frame src=kanan.html name=kanan  scrolling="yes" >
  </frameset>
  </frameset><noframes></noframes>
</html>
```

Source code (kanan.html)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>kanant</title>
  <link rel="stylesheet" href="mod2.php_files/style.css" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="3" cellspacing="2">
          <tbody></tbody></table>                    </td>
    </tr>
    </tbody></table>
    <p><strong><H2>Abstrak</H2>
    </strong></p>
      Keamanan sistem informasi berbasis Internet harus sangat diperhatikan, karena jaringan
komputer Internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim
```