ANALISIS DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN DIONAEA SEBAGAI PENUNJANG KEAMANAN JARINGAN (STUDI KASUS : LABOR FAKULTAS TEKNIK UNIKS)

SKRIPSI

Oleh :

NPM	**: 160210079**
NAMA	**: ROSI DERMAWATI**
JENJANG STUDI	**: STRATA SATU (S1)**
PROGRAM STUDI	**: TEKNIK INFORMATIKA**

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM KUANTAN SINGINGI

2020

ANALISIS DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN DIONAEA SEBAGAI PENUNJANG KEAMANAN JARINGAN (STUDI KASUS : LABOR FAKULTAS TEKNIK UNIKS)

SKRIPSI

DIAJUKAN SEBAGAI SALAH SATU SYARAT UNTUK MENCAPAI GELAR SARJANA PROGRAM STUDI TEKNIK INFORMATIKA

Oleh :

NPM	**: 160210079**
NAMA	**: ROSI DERMAWATI**
JENJANG STUDI	**: STRATA SATU (S1)**
PROGRAM STUDI	**: TEKNIK INFORMATIKA**

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM KUANTAN SINGINGI
2020

KATA PENGANTAR

Berkat rahmat Tuhan Yang Maha Esa, penulis dapat menyelesaikan Laporan Skripsi yang berjudul **"Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan (Studi Kasus Labor Fakultas Teknik UNIKS)"** sesuai dengan yang direncanakan. Selanjutnya penulis menyampaikan terima kasih kepada:

1. Bapak **Prof. Dr. H. Zulfan Sa'am, M.Si.** Selaku Ketua Yayasan Pendidikan Tinggi Islam Kuantan Singingi.
2. Ibu **Ir. Hj. Elfi Indrawanis, MM.** Selaku Rektor Universitas Islam Kuantan Singingi.
3. Ibu **Gusmulyani, ST., MT.** Selaku Dekan Fakultas Teknik Universitas Islam Kuantan Singingi.
4. Bapak **Elgamar, S.Kom., M.Kom.** Selaku Ketua Program Studi Teknik Informatika.
5. Bapak **Harianja, S.Pd., M.Kom.** Selaku Dosen Pembimbing 1.
6. Bapak **Elgamar , S.Kom., M.Kom.** Selaku Dosen Pembimbing 2.
7. Bapak **Jasri, S.Kom., M.Kom.** Selaku Kepala Labor Teknik tempat penulis membuat program.
8. Bapak **Hary Akbar, S.Kom.** Selaku Laboran Fakultas Teknik.
9. Bapak/Ibu Dosen Universitas Islam Kuantan Singingi yang telah banyak membantu penulis dalam menyelesaikan Skripsi ini.
10. Orang tua tercinta dan keluarga, yang telah memberikan do'a, semangat, dukungan dan motivasi selama ini.

11. Teman bar-bar **Mei Monica Utari.** Selaku teman yang telah menemani selama suka dan duka dalam pembuatan Skripsi ini. Jika tidak ada dia mungkin saya tidak bisa menyelesaikan Skripsi ini.
12. Terima kasih juga saya ucapkan kepada **Andika Maulana, S.Kom.** Selaku teman jauh yang tidak pernah bertemu yang membantu mencarikan referensi.
13. Semua pihak yang tidak dapat disebutkan satu per satu yang terlibat dalam penulisan Skripsi ini sehingga dapat selesai dengan baik.

Akhir kata kepada semua pihak yang memberikan bantuan baik moril maupun material, yang tidak dapat penulis sebutkan satu per satu yang telah membantu dalam penyusunan Skripsi ini. Serta tak lupa saran dan kritikan dari semua pihak dan penulis akan terima dengan senang hati. Semoga skripsi ini bermanfaat bagi pihak yang berkepentingan.

Telukkuantan, 30 Agustus 2020

ROSI DERMAWATI
NPM. 160210079

PERNYATAAN

Saya yang betanda tangan di bawah ini:

NPM	: 160210079
Nama	: ROSI DERMAWATI
Tempat/Tgl Lahir	: Talontam, 09 Juli 1997
Alamat	: Desa Talontam Kec. Benai Kab. Kuantan Singingi

Menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana komputer di suatu perguruan tinggi dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Telukkuantan, 27 Agustus 2020

ROSI DERMAWATI
NPM. 160210079

PERSETUJUAN SEMINAR SKRIPSI

NPM : 160210079

Nama : ROSI DERMAWATI

Jenjang Studi : Strata Satu (S1)

Program Studi : Teknik Informatika

Judul Skripsi : Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan (Studi Kasus : Labor Fakultas Teknik UNIKS)

Disetujui Oleh:

Pembimbing 1

HARIANJA, S.Pd, M.Kom Tanggal : 27 Agustus 2020
NIDN. 1017057702

Pembimbing 2

M. HASIM SIREGAR, S.Kom, M.Kom Tanggal : 27 Agustus 2020
NIDN. 1020019201

Mengetahui,
Ketua Prodi Teknik Informatika

ELGAMAR, S.Kom, M.Kom Tanggal : 27 Agustus 2020
NIDN. 1022108702

TANDA PENGESAHAN SKRIPSI

NPM : 160210079

Nama : ROSI DERMAWATI

Jenjang Studi : Strata Satu (S1)

Program Studi : Teknik Informatika

Judul Skripsi : Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan (Studi Kasus : Labor Fakultas Teknik UNIKS)

Dipertahankan Di Depan Tim Penguji Skripsi

Program Studi Teknik Informatika Fakultas Teknik UNIKS

Pada Tanggal : 31 Agustus 2020

Dewan Penguji

No	Nama	Jabatan	Tanda Tangan
1.	Gusmulyani, S.T, M.T	Ketua	
2.	Nofri Wandi Al-Hafiz, M.Kom	Sekretaris	
3.	Harianja, S.Pd, M.Kom	Pembimbing 1	
4.	M. Hasim Siregar, S.Kom, M.Kom	Pembimbing 2	
5.	Jasri, S.Kom, M.Kom	Penguji 1	
6.	Elgamar, S.Kom, M.Kom	Penguji 2	

Mengetahui,

Dekan,
Fakultas Teknik

GUSMULYANI, S.T, M.T
NIDN. 0007107301

Ketua,
Prodi Teknik Informatika

ELGAMAR, S.Kom, M.Kom
NIDN. 1022108702

ABSTRAK

Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah komputer. Banyak dijumpai komputer tidak meng*update* antivirusnya bahkan ada yang tidak memakai antivirus. Teknik pengamanan jaringan biasanya dengan memblokade serangan menggunakan *firewall* atau mendeteksi serangan dengan IDS *(Intruction Detection System)*, yang bertugas untuk menjaga dari serangan-serangan yang ada. Namun hanya dengan menggunakan IDS *administrator* jaringan akan kewalahan memeriksa setiap pemberitahuan yang diberikan oleh IDS. IDS ini bekerja hampir sama seperti antivirus, tidak mampu untuk bekerja dalam lingkungan terenkripsi atau lingkungan IPv6. Untuk itu diperlukan keamanan tambahan seperti *honeypot dionaea. Honeypot* merupakan sebuah sistem palsu yang dirancan untuk menjebak *malware*, seolah-olah yang diserang adalah sistem yang asli. Berdasarkan dari permasalahan ini maka akan dilakukan penelitian tentang Analisis dan Implementasi *Honeypot* Menggunakan *Dionaea* Sebagai Penunjang Keamanan Jaringan.

Kata Kunci : *Honeypot*, *Dionaea*, IDS, *Firewall, Malware.*

ABSTRACT

Lack of knowladge of computer user about system security problem is one of the couse of computer problems. There are many computers that don't update their antivirus and some even don't use an antivirus. Network security techniques usually block attack using a firewall or detect attack with IDS (Intruction Dectection System), which is in charge of guarding against aqisting attacks. However, by only using IDS the network administrator will be overwhelmed checking every notification given by IDS. This IDS works almost the same as an antivirus, unable to work in an encrypted environment or an IPv6 environment. For that, andditional security is needed such as a dionaea honeypot. A honeypot is fake system the signed to trap malware, as if it were a real system. Based on these problems, are research will be conducted on the Analysis on Implementation Of Honeypot Using Dionaea As Network Security Support.

Keywords : *Honeypot, Dionaea, IDS, Firewall, Malware*

KATA PENGANTAR

Berkat rahmat Tuhan Yang Maha Esa, penulis dapat menyelesaikan Laporan Skripsi yang berjudul **"Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan (Studi Kasus Labor Fakultas Teknik UNIKS)"** sesuai dengan yang direncanakan. Selanjutnya penulis menyampaikan terima kasih kepada:

1. Bapak **Prof. Dr. H. Zulfan Sa'am, M.Si.** Selaku Ketua Yayasan Pendidikan Tinggi Islam Kuantan Singingi.
2. Ibu **Ir. Hj. Elfi Indrawanis, MM.** Selaku Rektor Universitas Islam Kuantan Singingi.
3. Ibu **Gusmulyani, ST., MT.** Selaku Dekan Fakultas Teknik Universitas Islam Kuantan Singingi.
4. Bapak **Elgamar, S.Kom., M.Kom.** Selaku Ketua Program Studi Teknik Informatika.
5. Bapak **Harianja, S.Pd., M.Kom.** Selaku Dosen Pembimbing 1.
6. Bapak **M. Hasim Siregar, S.Kom., M.Kom.** Selaku Dosen Pembimbing 2.
7. Bapak **Jasri, S.Kom., M.Kom.** Selaku Kepala Labor Teknik tempat penulis meneliti.
8. Bapak **Hary Akbar, S.Kom.** Selaku Laboran Fakultas Teknik.
9. Bapak/Ibu Dosen Universitas Islam Kuantan Singingi yang telah banyak membantu penulis dalam menyelesaikan Skripsi ini.
10. Orang tua tercinta dan keluarga, yang telah memberikan do'a, semangat, dukungan dan motivasi selama ini.

11. Teman bar-bar **Mei Monica Utari.** Selaku teman yang telah menemani selama suka dan duka dalam pembuatan Skripsi ini. Jika tidak ada dia mungkin saya tidak bisa menyelesaikan Skripsi ini.
12. Terima kasih juga saya ucapkan kepada **Andika Maulana, S.Kom.** Selaku teman jauh yang tidak pernah bertemu yang membantu mencarikan referensi.
13. Semua pihak yang tidak dapat disebutkan satu per satu yang terlibat dalam penulisan Skripsi ini sehingga dapat selesai dengan baik.

Akhir kata kepada semua pihak yang memberikan bantuan baik moril maupun material, yang tidak dapat penulis sebutkan satu per satu yang telah membantu dalam penyusunan Skripsi ini. Serta tak lupa saran dan kritikan dari semua pihak dan penulis akan terima dengan senang hati. Semoga skripsi ini bermanfaat bagi pihak yang berkepentingan.

Telukkuantan, 28 Agustus 2020

ROSI DERMAWATI
NPM. 160210079

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Sistem komputer menjadi bagian yang sangat penting dan tidak dapat dipisahkan dalam dunia pendidikan. *Internet* merupakan jaringan komputer yang bersifat publik. Jaringan komputer yang terhubung ke *internet* akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan. *Malicious Software* (*Malware*) merupakan program komputer yang diciptakan dengan tujuan mencari kelemahan atau bahkan merusak sistem operasi[1] . *Malware* dalam bentuk *virus, worm* dan *trojan* merupakan ancaman utama bagi keamanan sistem jaringan komputer.

Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah terhadap komputer. Sering dijumpai komputer yang program anti virusnya tidak di *update*, atau bahkan tidak dilengkapi dengan program antivirus sama sekali. Hal tersebut menyebabkan komputer atau *host* dapat terinfeksi *malware* tanpa sepengetahuan dari pengguna. Kemudian *malware* tersebut dapat menyebar ke komputer lainnya dalam jaringan dan pada akhirnya dapat merugikan banyak pihak.

Teknik pengamanan jaringan biasanya dengan memblokade serangan dengan *firewall* atau mendeteksi serangan yang ada dengan IDS (*Intrusion Detection System*) yang bertugas untuk menjaga dari serangan-serangan yang ada. IDS sendiri adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau

jaringan[2] . Namun IDS sendiri tidak serta merta dapat menahan serangan para penyerang. Selain menggunakan cara konvensional tersebut pengamanan sistem jaringan dapat menggunakan *honeypot*. *Honeypot* adalah sebuah sistem palsu yang dirancang untuk menjebak penyerang, seolah-olah yang diserang adalah sistem yang asli[3] . Honeypot akan memberikan data palsu apabila ada hal aneh yang akan masuk ke dalam sistem atau *server*. Salah satu yang didapat menggunakan *honeypot* dalam keamanan jaringan adalah informasi bagaimana seorang penyerang dapat menerobos dan apa yang sudah dilakukannya[4] . Sehingga seorang *administrator* jaringan dapat melihat dengan nyata informasi suatu serangan. *Honeypot* ini sangat penting untuk menjadi suatu perangkat tambahan demi meminimalisir serangan yang terjadi ke dalam sistem.

Dionaea adalah sebuah alat yang digunakan untuk menjebak penyerang dengan memanfaatkan kerentanan *malware* terhadap layanan atau layanan pada suatu jaringan[5] . *Dionaea* termasuk kategori dari *low-interaction honeypot* terbaru yang merupakan suksesor dari *Nephentes*. *Honeypot dionaea* dengan lisensi *open source* merupakan salah satu varian dari beberapa *low-interactioan honeypot* seperti *Nephentes*, *HoneyD* dan lain-lain yang termasuk kategori *honeypot low-interaction*. Karena *dionaea* dapat menentukan *host* yang terinfeksi *malware*, maka tindakan pada *host* yang terinfeksi dapat dilakukan agar dapat dihentikan penyebaran *malware* tersebut ke *host* lain dalam jaringan.

Laboratorium Aplikasi Fakultas Teknik UNIKS banyak terdapat komputer yang terhubung ke dalam jaringan internet. Hampir semua aktivitas yang dilakukan menggunakan jaringan internet. Tetapi keamanan yang diterapkan masih secara konvesional.

Berdasarkan uraian di atas penulis melihat perlu dilakukan penelitian lebih lanjut terhadap sistem keamanan jaringan terutama labor Fakultas Teknik UNIKS dari serangan *malware* yang dapat merusak serta merugikan. Penelitian ini juga dapat menjadi acuan atau gambaran jika nantinya terutama Fakultas Teknik memiliki sebuah server. Untuk itu penulis menarik judul dalam penelitian ini "Analisis dan Implementasi *Honeypot* Menggunakan *Dionaea* Sebagai Penunjang Keamanan Jaringan".

1.2. Identifikasi Masalah

Berdasarkan latar belakang masalah di atas maka identifikasi masalah dalam penelitian ini adalah :

1. Penggunaan teknik keamanan jaringan dengan cara memblokade serangan dengan *firewall* atau mendeteksi serangan yang ada dengan IDS (*Intrusion Detection System*) tidak serta merta dapat menahan serangan dari para penyerang/*malware.*
2. Penggunaan metode IDS (*Intrusion Detection System*) hanya memberikan notifikasi yang dianggap mencurigakan tanpa mengetahui notifikasi informasi yang diberikan asli atau tidak, sehingga tugas *administrator* jaringan lebih rumit.

1.3. Rumusan Masalah

Berdasarkan identifikasi masalah di atas dapat dirumuskan permasalahannya yaitu :

1. Bagaimana mengimplementasikan *honeypot dionaea* sebagai solusi dalam mengatasi masalah pada keamanan jaringan terutama dalam mendapatkan *malware*?
2. Bagaimana kinerja *honeypot dionaea* dapat melakukan analisa sederhana *malware* dengan menggunakan bantuan *software* berbasis *open source*?

1.4. Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

1. Hanya membahas masalah analisis dan implementasi *honeypot dionaea* dan tidak membahas *firewall* dan IDS.
2. Menggunakan *Oracle VM VirtualBox* sebagai perangkat lunak virtualisasi.
3. Penelitian ini dilakukan di labor Fakultas Teknik UNIKS.

1.5. Tujuan dan Manfaat Penelitian

1.5.1. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Berhasil mengimplementasikan *honeypot dionaea* di salah satu komputer labor.
2. Penganalisaan serangan atau *malware* yang dilakukan oleh seorang *administrator* jaringan dengan *honeypot dionaea* menjadi lebih terorganisir dan tepat sasaran.

1.5.2. Manfaat Penelitian

Dengan melakukan penelitian ini diharapkan bisa memberikan manfaat antara lain :

1. Dengan menerapkan *honeypot dionaea* sebagai teknik keamanan jaringan dapat membantu *administrator* jaringan mengetahui perilaku *malware.*
2. Informasi data *malware* dapat digunakan oleh *administrator* jaringan untuk mempelajari perilaku *malware* serta pencegahan yang dapat dilakukan

.

1.6. Sistematika Penulisan

Penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab ini berisi latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Dalam bab ini berisi tentang penjelasan dan penjabaran teori-teori yang akan dipergunakan untuk mendukung materi secara *detail,* dapat definisi-definisi yang langsung yang berkaitan dengan masalah diteliti, tinjauan penelitian sebelumnya serta aplikasi yang

digunakan.

BAB III : METODE PENELITIAN

Dalam bab ini menjelaskan cara pelaksanaan kegiatan penelitian, mencakup cara pengumpulan data, alat yang digunakan dan cara analisa data.

BAB IV : ANALISA DAN PERANCANGAN SISTEM

Dalam bab ini akan diuraikan gambaran mengenai sistem pendukung objek yang diteliti dan perancangan berkas. Pada bab ini juga akan dilaporkan secara *detail* rancangan terhadap penelitian yang dilakukan.

BAB V : IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini berisi tentang implementasi secara men*detail,* serta memberikan hasil pengujian yang dilakukan secara menyeluruh.

BAB VI : PENUTUP

Untuk bab ini berisi kesimpulan dan saran-saran untuk perbaikan dan pengembangan terhadap sistem yang telah dibuat.

BAB II

TINJAUAN PUSTAKA

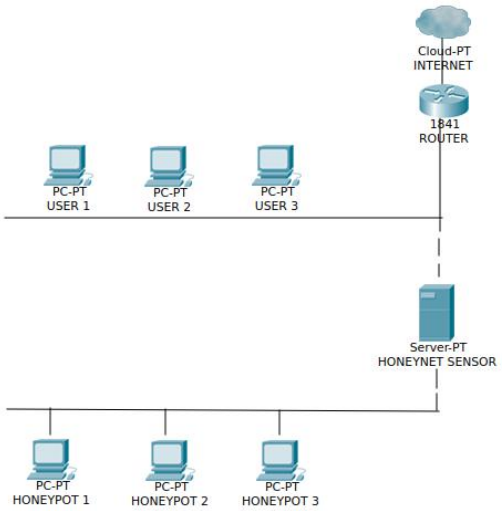
2.1. Teoritis

Untuk memudahkan pemahaman tentang apa yang akan dilakukan pada tugas akhir ini, berikut ini akan dipaparkan konsep dan teknologi apa saja yang akan digunakan. Adapun teknologi yang akan dilakukan pada tugas akhir ini adalah sebagai berikut :

2.1.1. Ubuntu

Menurut Akbar Ubuntu adalah distro *linux* turunan *debian* yang dikembangkan dengan tujuan utama menjadi distro *linux desktop* yang mudah digunakan dengan rilis stabil setiap 6 bulan sekali[6] . *Ubuntu* berasal dari kata dalam bahasa Afrika kuno ubuntu yang maknanya kemanusiaan untuk semua (*humanity towards others*).*Ubuntu* sangat populer karena kemudahannya dan dukungan komunitas yang besar.*Ubuntu* berkomitmen akan selalu gratis dan didistribusikan sebagai perangkat lunak bebas sumber terbuka (*free and open source software*). *Ubuntu* populer dengan sistem manajemen paket yang sangat anggun bernama apt (*Advanced Package Tool*) yang diwarisi dari *debian*. Sistem manajemen paket ini otomatis mencarikan dependensi untuk suatu aplikasi yang akan diinstal dan menginstalkannya dari repositori ke sistem. *Ubuntu* selain memiliki apt yang amat praktis, juga mewarisi dpkg (*DebianPackager*) dan GDebi untuk mengelola program (paket) di dalam sistem.

2.1.2. Honeypot



Gambar 2.1.2. Arsitektur *Honeypot*

Secara singkat *honeypot* merupakan sebuah sistem yang di bangun menyerupai/persis dengan sistem yang sesungguhnya, dengan tujuan agar para *attacker* teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut. Saat ini *honeypot* tidak hanya berfungsi atau bertujuan untuk menjebak *attacker* untuk melakukan serangan ke *server* asli, namun *honeypot* juga bermanfaat untuk para sistem *administrator* atau *security analyst*, untuk menganalisa aktifitas apa saja yang dilakukan oleh *attacker/malware* yang terdapat di dalam sistem *honeypot* tersebut.Secara umum terdapat dua tipe *honeypot* yaitu:

1. *Low Interaction Honeypot*

Low Interaction Honeypot merupakan jenis *honeypot* yang memiliki karakteristik lebih mudah dan cepat untuk diterapkan, hal tersebut dikarenakan *honeypot* jenis ini hanya menyediakan tiruan dari layanan tertentu saja, tipe *honeypot* yang dibuat untuk mensimulasikan *service* (layanan) *FTP, Telnet, HTTP,* dan *service* lainnya. *Honeypot* yang termasuk ke dalam *low interaction*

diantaranya *kippo, honeyd, dionaea*.

2. *High Interaction Honeypot*

Tipe *honeypot* yang menggunakan keseluruhan *resource* sistem, dimana *honeypot* yang dibangun nanti benar-benar persis seperti sistem yang asli. *Honeypot* jenis ini bisa berupa satu keseluruhan sitem operasi beserta aplikasi yang berjalan didalamnya. *Honeypot* yang termasuk ke dalam *high interaction* adalah hihat.

2.1.3. Dionaea

Dionaea adalah sebuah *low interaction honeypot* yang memiliki tujuan untuk mendapatkan *copy* dari *malware[7]* . *Dionaea* menggunakan bahasa pemrograman *python* sebagai bahasa *scripting,libemu*untuk mendeteksi *shellcode,* mendukung Ipv6 dan TLS. Perangkat lunak (*software*) cenderung memiliki *bug*, yang seringkali dapat dieksploitasi oleh pihak lain untuk memperoleh informasi atau keuntungan.

Dionaea memiliki kemampuan untuk mendeteksi dan mengevaluasi payload agar dapat memperoleh salinan malware.Dalam mendeteksi payloaddionaea menggunakan libemu.Setelah dionaea memperoleh lokasi berkas yang diinginkan penyerang agar diunduh dari shellcode, dionaeaakan mencoba untuk mengunduh berkas tersebut. Protokol untuk mengunduh berkas tersebut menggunakan TFTP dan FTP yang diimplementasikan menggunakan bahasa pemrograman python (tftp.py dan ftp.py) sebagai bagian dari dionaea. Berkas diunduh melalui HTTP yang dilakukan dalam modul curl yang memanfaatkan libcurl HTTP.

2.1.4. IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System)

Fungsi IDS adalah untuk menangkap setiap aktivitas yang terjadi pada jaringan dan juga karena pada umumnya IDS mempunyai *signature database* maka IDS dapat memberikan informasi yang lengkap dari suatu koneksi yang terjadi[2] . Pada saat ini ada beberapa *intrusion* IDS yang umum digunakan pada jaringan, salah satunya *snort.*

IPS merupakan jenis metode pengamanan jaringan baik *software* atau *hardware* yang dapat memonitor aktivitas yang tidak diinginkan atau *intrusion* dan dapat langsung bereaksi untuk mencegah aktivitas tersebut[8] . IPS merupakan pengembangan dari IDS. Sebagai pengembangan dari teknologi *firewall* IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau *pattern,* tidak hanya berdasarkan *port* atau *IP Address* seperti *firewall* pada umumnya.

2.1.5. OSI Layer

Model OSI menerapkan konsep yang dikenal dengan enkapsulasi. Enkapsulasi adalah metode membungkus data dari suatu lapisan model OSI dalam struktur data baru sehingga setiap lapisan model OSI hanya akan melihat dan berususan dengan formasi yang dibutuhkan untuk dengan benar menangani dan memberikan data pada jaringan komputer[9].

Layer	Fungsi	Contoh Protokol
Aplication	Menyediakan servis bagi berbagai aplikasi network	NNTP, H7, Modbus, SIP, SSI, DHCP, FTP, Gopher, HTTP, NFS, NTP. RTP, SMPP, SMTP, Telnet
Presentation	Mengatur konversi dan translasi berbagai format data, seperti kompresi data dan enkripsi data	TDI, ASCII, EBCDIC, MIDI, MPEG, ASCII7
Session	Mengatur sesi (*session*) yang meliputi estabilishing (memulai sesi), maintaining (mempertahankan sesi) dan terminating (mengakhiri sesi) antar entitas yang dimiliki oleh presentation layer	SQL, X Windows, DNS, NetBIOS, ASP, SCP, OS Scheduling, RPC, NFS, ZIP
Transport	Menyediakan end to end communication protocol. Layer ini bertanggung jawab terhadap "keselamatan data" seperti mengatur flow control (kendali aliran data), error detection (deteksi error) dan correction (koreksi), data secuencing (urutan data) dan size of the packet (ukuran data)	TCP, SPX, UDP, SCTP, IPX
Network	Menentukan rute yang dilalui oleh data. Layer ini menyediakan logical addressing (pengalamatan logika) dan path determination (penentuan rute tujuan)	IP, ICMP, IPSec, ARP. RIP, IGRP, BGP, QSPF, NBF, Q.931
Data Link	Menentukan pengalamatan fisik (hardware address), error notifikasi (pendeteksi error), frame flow control (kendali aliran frame) dan topologi aliran network Ada dua sub layer pada data link, yaitu Logical Link Control (LLC) dan Media Access Control (MAC) LLC mengatur komunikasi, seperti error notification dan flow control. Sedangkan MAC mengatur pengalamatan fisik yang digunakan dalam proses komunikasi antar adapter	802.3 (Ethernet) 802.11 a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, CDP, HDP, FDDI, Fibre Channel Frame Relay, SDLC, HDLC, ISL, PPP Q.921, Token Ring
Physical	Layer ini menentukan masalah kelistrikan / gelombang / medan dan berbagai prosedur / fungsi yang berkaitan dengan link fisik, seperti besar tegangan / arus listrik, panjang maksimal media transmisi, pergantian fasa, jenis kabel dan konektor	RS.232, V.35, V.34, L430, L.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, DSL, 802.11a/b/g/n PHY, Hub, Repeater, Fibre, Optics

Gambar 2.1.5. OSI Layer [10]

2.1.6. VirtualBox

Oracle VM VirtualBox adalah paket perangkat lunak virtualisasi *open source* x86 lintas *platform*, yang sekarang dikembangkan oleh *Oracle Corporation* sebagai bagian dari keluarga produk virtualisasi[11] .

VirtualBox adalah *hosted hypervisor*. Pada tingkat yang sangat besar, *VirtualBox* secara fungsional identik pada semua *platform host, file* dan *image*. Hal ini memungkinkan untuk menjalankan VM yang dibuat di satu *host* pada *host* lain dengan sistem operasi *host* yang berbeda, misalnya VM dibuat pada *Windows* dan kemudian dijalankan di *Linux*. *VirtualBox* termasuk jenis virtualisasi penuh dan dapat membangun bentuk jaringan yaitu LAN (*Local Area Network*) yang tidak membutuhkan perangkat yang banyak. *VirtualBox* ini adalah solusi virtualisasi untuk *hardware* x86 maupun

x64 yang *extensi* virtualisasi (Intel VT atau AMD-V)[4] .

2.1.7. Malware

Malware yang merupakan singkatan dari *malicious software* adalah sebuah program atau perangkat lunak yang diciptakan untuk tujuan menyusup, mengganggu atau bahkan merusak sistem operasi pada suatu perangkat komputer.Program ini dapat menjalankan suatu perintah tertentu pada perangkat yang disusupinya.Jika salah satu perangkat sudah terinfeksi program *malware*, maka perangkat tersebut dapat menjalankan atau melakukan sesuatu tanpa sepengetahuan pemilik dengan tujuan tidak baik. Contoh dari *malware* adalah *Virus, Worm, Wabbit, Keylogger, Browser Hijacker, Trojan Horse, Spyware, Backdoor, Dialer, Exploit, dan Rootkit[12]* .

2.1.8. DOS *(Denial Of Service) Attack*

J.D. Howard mendefinisikan DOS adalah apabila *hardware, software* dan data komputer tidak dapat terjaga ketersediaannya, maka produktivitas operasional jadi turun, walaupun tidak ada kerusakan yang terjadi[13] .

Denial of Service dapat mencakup kedua keadaan tersebut yang secara disengaja maupun tidak disengaja melakukan serangan kepada ketersediaan sistem (*system availability*). Perpektif yang muncul tanpa melihat sebab yang terjadi adalah apabila layanan diibaratkan tersedia padahal tidak ada sehingga mengakibatkan layanan *denied* (tidak ada). Suatu serangan bagaimanapun adalah suatu tindakan disengaja.*Denial of Service attack* diyakini berlangsung ketika mengakses ke komputer atau *resource* jaringan dengan sengaja di*blocked* atau hak aksesnya diturunkan dari *user* lain. Serangan ini tidak perlu merusak data secara langsung atau permanen (walaupun mereka dapat melakukannya), tetapi mereka dengan sengaja berkompromi (mengganggu) ketersediaan dari *resource*. Macam serangan DoS *attack* umumnya melalui jaringan, dimana target utama dari serangan adalah *website* yang popouler seperti *Ebay, Amazon, Buy.com, CCN.com dan Yahoo.com.*

Umumnya *site-site* tersebut mempunyai banyak *hardware* yang mereka gunakan, sehingga *attacker*akan bekerja keras untuk menyerang. *Website* normalnya terdiri dari beberapa *web-server* dengan sistem *load balancing* dan memiliki koneksi jaringan *multi megabit*. Sebagai konsekuensi *attacker* harus menemukan jalur baru untuk menaklukkan sistem.*Attacker* tidak menggunakan satu *host* dalam penyerangan mereka, tetapi menggunakan beberapa ratus bahkan ribuan komputer untuk melakukan serangan yang terkoordinir. Jenis serangan seperti ini disebut *Distributed Denial of Service attack* (DDoS *attack*).

2.2. Penelitian Terdahulu

Penelitian terdahulu merupakan acuan/gambaran bagi penulis untuk melakukan kegiatan penelitian selanjutnya yang mana pembahasannya hampir serupa dengan penelitian yang akan penulis lakukan. Berikut ini tabel beberapa penelitian terdahulu yang sudah dijurnalkan:

Tabel 2.2. Penelitian Terdahulu

No	Nama Penulis	Judul	Hasil
1.	Cahyanto, T. A., Oktavianto, H., & Royan, A. W. (2017)	Analisis dan implementasi *honeypot* menggunakan *dionaea* sebagai penunjang keamanan jaringan.	Dari hasil pengujian dapat disimpulkan bahwa *Dionaea* dapat digunakan sebagai *server* palsu atau *server* tiruan sehingga dapat melindungi *server* asli ketika *server* tiruan tersebut mengalami serangan. Pengujian *server* tiruan tersebut berbasis *Dionaea* menggunakan *Metasploit Framework*, dan melibatkan tiga teknik *exploit* yaitu MS04_011_LSASS,MS03_026_DCOM dan MySQL_Payload. Berdasarkan

			simulasi serangan yang sudah dikerjakan, dapat diketahui bahwa penggunaan *honeypot* dapat menunjang keamanan jaringan, namun *honeypot* tidak dapat melindungi sistem operasi khususnya *windows*. Ditemukan banyak kelemahan pada sisi aplikasi, sehingga sisi kelemahan pada aplikasi tersebut dapat dimanfaatkan oleh penyerang untuk menguasai sistem seperti yang sudah ditunjukkan pada pengujian serangan.
2.	Alfiansyah, F.B. (2015)	Implementasi Monitoring *Autonomous Spreading* Malware di ITS-NET dengan *Dionaea* dan *Cockoo*	1. Sensor *honeypot Dionaea* telahberhasil diimplementasikandi jaringan ITS-Net dan setelahdijalankan dalam waktu 4 bulan telah berhasil menangkap 362 *binaries autonomous spreading malware.* 2. *Toolssandbox Cuckoo* telah berhasil diimplementasikan pada sebuah komputer di ITS-Net sehingga dapat digunakan sebagai alat identifikasi jenis dan perilaku *malware.* 3. Dari hasil identifikasi autonomous spreding malware yangada di jaringan ITS-Net didapatkan empat kategori *malware* yaitu: *trojan, worm, botnet* dan *spyware.*

BAB III

METODE PENELITIAN

3.1. Uraian Tempat Penelitian

3.1.1. Sejarah Singkat Tempat Penelitian

Pendirian Universitas diawali dengan diskusi pimpinan, beberapa dosen dan staf STIP-US dan STT-US yang kemudian direspon oleh Pemerintah Daerah melalui Pidato Bupati pada Kuliah Umum September 2008. Tahun 2009 berkembang ide bukan hanya penyatuan dua Sekolah Tinggi yang berada dalam naungan Yayasan Perguruan Tinggi Kuantan Singingi tetapi juga menyatukan STAI yang berada di bawah Yayasan Pendidikan Tinggi Islam Kuantan Singingi. Untuk mempermudah dan efisiensi pengelolaan, maka perlu penyatuan Sekolah Tinggi yang ada di Kabupaten Kuantan Singingi ke dalam bentuk Universitas yang dikelola oleh satu Yayasan.

Perguruan Tinggi yang akan didirikan berbentuk Universitas dengan nama Universitas Islam Kuantan Singingi Merupakan gabungan tiga Sekolah Tinggi yang ada. Ketiga Sekolah Tinggi dimaksud berada dalam naungan dua Yayasan. Yayasan Perguruan Tinggi Kuantan Singingi mengelola Sekolah Tinggi Ilmu Pertanian Unggulan Swarnadwipa (STIP-US) dan Sekolah Tinggi Teknologi Unggulan Swarnadwipa (STT-US) dengan akta notaris Tito Utoyo, SH, tanggal 30 Juni 2000, nomor 92 dan berhasil diperoleh izin tanggal 5 Juli 2001, dengan No.Izin : 66/D/O/2001. Sedangkan Yayasan Pendidikan Tinggi Islam Kuantan Singingi menaungi Sekolah Tinggi Agama Islam (STAI) dengan Akta Notaris Tajib Raharjo SH, tanggal 24 Mei 2002 Nomor 152 dan izin operasional atas

nama Menteri Agama RI, Koordinator Perguruan Tinggi Agama Islam (Kopertais) Wilayah XII Riau-Kepri, tanggal 21 September 2002 nomor: 12/ XII/ K/2002.

3.1.2. Struktur Organisasi

Gambar 3.1.2. Stuktur Organisasi Labor Teknik UNIKS

Berdasarkan gambar 3.1.2, otoritas tertinggi adalah jabatan Kepala Labor yang bertanggung jawab atas labor Fakultas Teknik UNIKS. Untuk membantu menjalankan tugas Kepala Labor dibantu oleh Laboran yang bertugas secara khusus menangani hal-hal yang bersifat teknis operasional.

3.1.3. Tugas Pokok dan Fungsi dari Struktur Organisasi

3.1.3.1. Tugas Pokok Kepala Labor

1. Memantau kinerja bawahan.
2. Memastikan labor Fakultas Teknik terkelola dengan baik.

3.1.3.2. Tugas Pokok Laboran

1. Bertanggung jawab terhadap penginstalan aplikasi yang dibutuhkan untuk proses pembelajaran.
2. Melakukan pengecekkan secara berkalaterhadap seluruh komputer di labor Fakultas Teknik UNIKS.

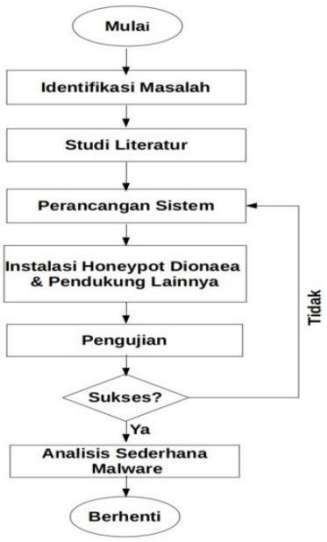
3. Melakukan perawatan/*maintenance* terhadap infrastuktur jaringan.

3.1.4. Fungsi Struktur Organisasi

1. Kejelasan dalam tanggung jawab.
2. Kejelasan dalam kedudukan.
3. Kejelasan dalam uraian tugas.

3.2. Diagram Alur Penelitian

Secara garis besar diagram alur dalam penelitian ini dibagi dalam beberapa tahapan. Pada gambar 3.2 menjelaskan metodologi penelitian dalam bentuk alur proses.



Gambar 3.2. Diagram Alur Penelitian

3.2.1. Identifikasi Masalah

Langkah pertama yang dilakukan dalam penelitian ini adalah menentukan identifikasi masalah, tujuan dan manfaat.

3.2.2. Studi Literatur

Studi literatur ini perlu dilakukan sebagai dasar dalam penelitian ini.Studi literatur dilakukan dengan mencari sumber-sumber referensi seperti jurnal-jurnal penelitian yang membahas atau berkaitan dengan *Honeypot Dioneaea* dan *Malware.*

3.2.3. Perancangan Sistem

Pada tahap ini, peneliti akan merancang sistem agar sesuai dengan kebutuhan dan tujuan yang diinginkan. Ada beberapa hal yang perlu diperhatikan dalam proses perancangan sistem ini yaitu menentukan spesifikasi *hardware, software* yang sesuai dan menentukan dimana posisi peletakan *Honeypot Dionaea.* Dalam hal ini melibatkan pihak dari labor Fakultas Teknik UNIKS.

3.2.4. Instalasi *Honeypot Dionaea*& Pendukung Lainnya

Pada tahap ini akan dilakukan penginstalan dan konfigurasi *Honeypot Dionaea* dan aplikasi pendukung lainnya.

3.2.5. Pengujian

Pada tahap ini, setelah *Honeypot Dionaea* selesai diinstal dan dikonfigurasi pengimplementasian dan pengambilan data dapat dilakukan. Sistem ini akan dipasang pada *IP public* dan dijalankan selama beberapa bulan untuk mendapatkan *malware.*

3.2.6. Analisa Sederhana *Malware*

Pada tahap ini, akan dilakukan identifikasi secara sederhana *malwar*e yang telah didapatkan sebelumnya di virustotal.com.

3.3. Teknik Mengumpulkan Data

Teknik pengumpulan data dan informasi yang penulis gunakan dalam penelitian ini adalah sebagai berikut:

1. Studi Pustaka

   Teknik pengumpulan data dan informasi tahap ini yaitu dengan cara mempelajari jurnal-jurnal yang terkait dengan penelitian, serta referensi dari media internet lainnya yang dapat dijadikan sebagai acuan dalam penelitian ini.

2. Wawancara

   Teknik pengumpulan data dan informasi tahap ini dilakukan dengan melakukan tanya jawab langsung melalui media sosial kepada Laboran Fakultas Teknik Universitas Islam Kuantan Singingi yang berkaitan langsung dengan masalah penelitian.

3.4. Rencana Jadwal Penelitian

Tabel 3.4. Rencana Jadwal Penelitian

No.	Kegiatan	Februari	Maret	April	Mei	Juni	Juli	Agustus
1.	Pengajuan Judul							
2.	Pengumpulan Data							
3.	Pembuatan Proposal							
4.	Seminar Proposal							
5.	Proses Bimbingan Skripsi							
6.	Sidang Skripsi							

BAB IV

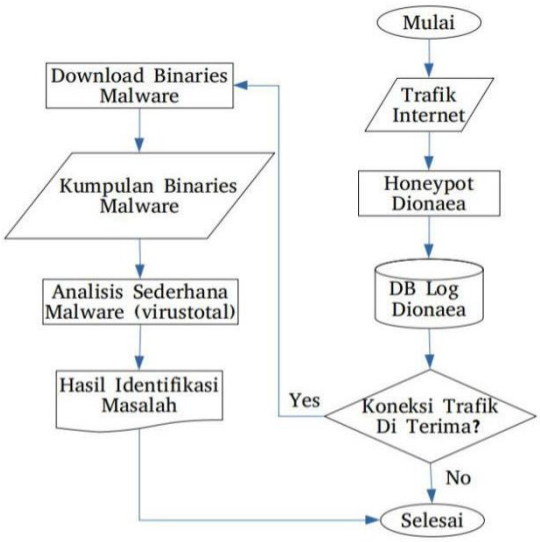
ANALISA DAN HASIL PERANCANGAN SISTEM

Pada bab ini akan membahas analisa dan perancangan sistem. Perancangan sistem ini terdiri dari beberapa tahap, yaitu: *flowchart* cara kerja sistem, *flowchart* tahapan konfigurasi, topologi jaringan yang ada di labor Fakultas Teknik UNIKS, tahapan pembangunan sistem, tahapan analisis sederhana *malware,* spesifikasi *hardware* dan metode pengambilan data.

4.1. *Flowchart* Cara Kerja Sistem

Pada tahap ini akan dijelaskan bagaimana cara kerja sistem. Desain *flowchart* cara kerja sistem terbagi menjadi dua bagian, yaitu: *flowchart* cara kerja sistem *honeypot dionaea* + virus total dan *honeypot dionaea.*

4.1.1. *Honeypot Dionaea* + virustotal

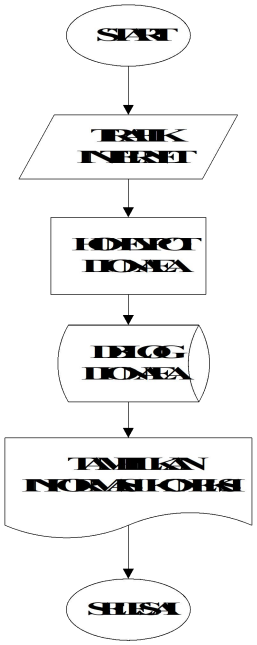


Gambar 4.1.1. Cara Kerja *Honeypot Dionaea* + virustotal

Pada gambar 4.1.1.menunjukkan*flowchart* cara kerja sistem *honeypot dionaea* + virustotal yang terdiri dari 8 langkah berikut ini:

1. Trafik jaringan internet yang masuk ke dalam sistem akan ditangkap oleh sensor *honeypot.*
2. *Honeypot dionaea* akan memproses semua trafik jaringan yang masuk ke dalam sistem.
3. Informasi masuk yang telah diterima dan diproses oleh *dionaea* akan disimpan ke dalam *database log dionaea.*
4. Setiap trafik jaringan internet yang masuk akan dicek, apakah statusnya diterima/ditolak. Apabila statusnya ditolak maka proses akan berhenti.
5. Apabila statusnya diterima, *dionaea* akan melanjutkan proses *download binaries malware.*
6. *Folder binaries* akan menyimpan data *binaries malware* yang telah berhasil ter-*download.*
7. Data *binaries malware* akan diproses menggunakan portal virustotal untuk dilakukan identifikasi jenis dan perilaku *malware.*
8. Dari analisis sederhana menggunakan virustotal akan menghasilkan laporan yang menunjukkan jenis dan perilaku *malware* serta antivirus yang dapat mendeteksi jenis *malware* tersebut.

4.1.2. Honeypot Dionaea



Gambar 4.1.2. Cara Kerja *Honeypot Dionaea*

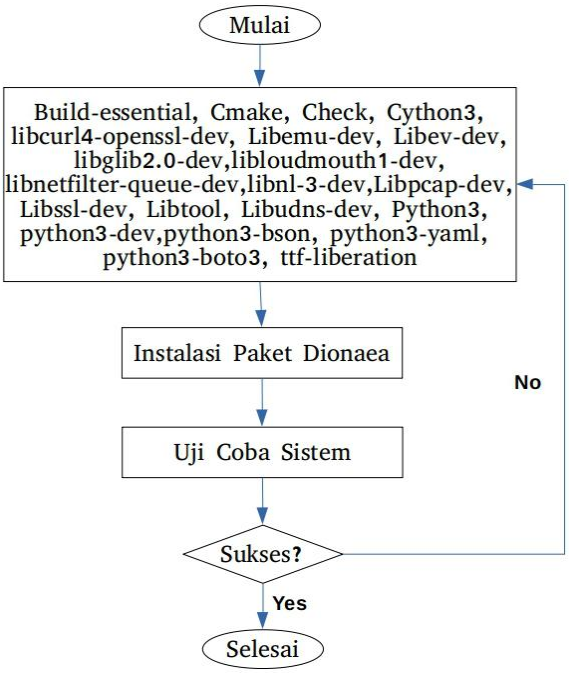
Pada gambar 4.1.2.menunjukkan desain *flowchart* cara kerja sistem *honeypot dionaea*yang terdiri dari 5 langkah berikut ini:

1. Trafik jaringan internet yang masuk ke dalam sistem akan ditangkap oleh sensor *honeypot*.
2. *Honeypot dionaea* akan memproses semua trafik jaringan yang masuk ke dalam sistem.
3. Informasi masuk yang telah diterima dan diproses oleh *dionaea* akan disimpan ke dalam *database log dionaea.*
4. *Database log dionaea* akan menyimpan koneksi di tabel *connections* menggunakan *sqlite3.*

4.2. *Flowchart* Tahapan Konfigurasi

Dalam mempermudah melakukan tahapan konfigurasi sistem, maka dibuatlah tahapan konfigurasi berbentuk *flowchart. Flowchart* tahapan konfigurasi akan dibuat menjadi 2 bagian sesuai dengan kebutuhan dalam penelitian yaitu: desain *flowchart honeypot dionaea*.

4.2.1. Honeypot Dionaea



Gambar 4.2.1.*Flowchart Konfigurasi Dionaea*

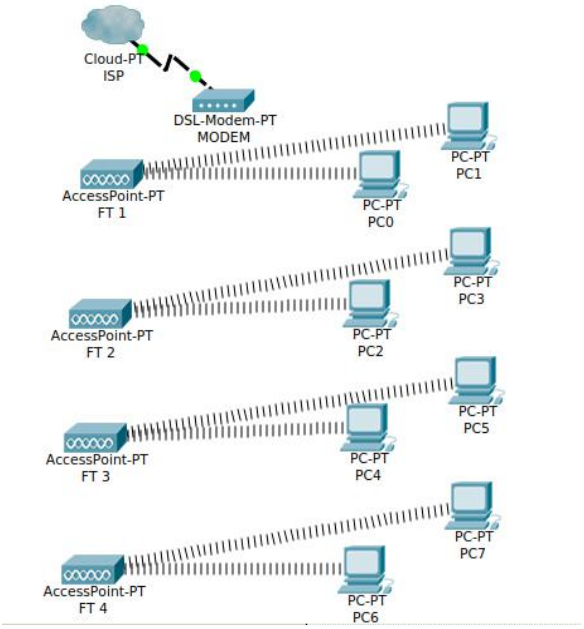
Pada gambar 4.2.1.menunjukkan*flowchart* konfigurasi *dionaea* yang terdiri dari 6 langkah berikut ini:

1. Konfigurasi dimulai dengan melakukan instalasi paket-paket *library* pendukung yang dibutuhkan oleh *dionaea* seperti: *Build-essential, Cmake, Check, Cython3, libcurl4-openssl-dev, Libemu-dev, Libev-dev, libglib2.0-dev,libloudmouth1-dev, libnetfilter-queue-dev,libnl-3-dev,Libpcap-dev, Libssl-dev, Libtool, Libudns-dev, Python3, python3-dev,python3-bson, python3-yaml,*

python3-boto3, ttf-liberation.

2. Setelah semua paket *library* pendukung berhasil diinstal dilanjutkan dengan instalasi paket *dionaea.*
3. Setelah semua *library* pendukung selesai diinstal, uji coba sistem untuk melihat apakah sistem sudah bisa berjalan dengan baik atau belum.
4. Jika sistem masih ditemukan *error* atau belum berjalan dengan baik maka proses konfigurasi harus diulang dari tahapan penginstalan paket *library* pendukung.
5. Apabila sistem sudah berjalan dengan normal maka tahapan konfigurasi selesai.

4.3. Topologi Jaringan



Gambar 4.3 Topologi Jaringan Labor Komputer

Access Point yang dipakai oleh Fakultas Teknik menggunakan teknologi WISP *(Wireless Internet Service Provider). Access Point* ini terhubung secara

wireless ke modem.

Dionaea diletakkan di depan *gateway* supaya koneksi yang ditangkap merupakan trafik murni tanpa adanya *filter* dari *gateway.* Sensor *honeypot dionaea* dipasang pada sebuah komputer yang akan terhubung secara *wireless* ke Access *Point*. Sensor *honeypot dionaea* sengaja diletakkan di luar *firewall* dengan menggunakan IP publik sehingga dapat menerima trafik jaringan dari manapun.

4.4. Spesifikasi *Hardware*

*Honeypot dionaea*akan diinstal di sebuah komputer dengan spesifikasi sebagai berikut:

1. RAM 4GB.
2. HDD 1TB .
3. CPU Intel(R) Core(TM) i5-7400T @2.40 GHz
4. OS Windows 10 Home SL.
5. ODD DVDRW.

4.5. Metode Pengambilan Data

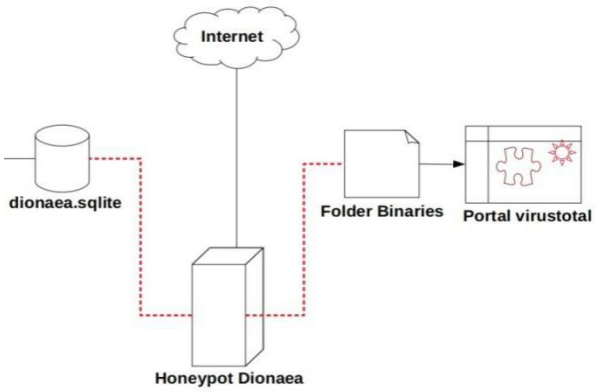
Berikut ini adalah metode pengambilan data:

1. *Dionaea* diinstal pada sebuah komputer.
2. Komputer yang telah terinstal *dionaea* dipasang di labor jaringan Fakultas Teknik UNIKS dengan IP publik kemudian dijalankan.
3. Komputer *dionaea* akan dijalankan 4 minggu untuk memperoleh hasil data *malware.*
4. Pada *dionaea*, data *log* disimpan di dalam *database sqlite3* dengan nama

dionaea.sqlite.

5. *Malware* yang telah ter-*download* akan tersimpan didalam folder "/opt/dionaea/var/lib/dionaea/binaries". Selanjutnya isi didalam *folder binaries* akan disalin ke portal virustotal untuk dilakukan penganalisaan.

4.6. Pembangunan Sistem



Gambar 4.6 Alur Pembangunan Sistem

Berdasarkan gambar di atas, komputer sensor *honeypot dionaea* diletakkan di labor jaringan Fakultas Teknik UNIKS dan dihubungkan ke internet dengan menggunakan IP publik. IP publik sengaja dipilih supaya sensor *honeypot dionaea* bisa melakukan *capture* trafik yang masuk dari manapun. Segala bentuk aktifitas atau trafik jaringan internet yang diterima oleh sensor *honeypot dionaea* akan tersimpan dalam *file database log (dionaea.sqlite).*

Data *malware* yang telah berhasil ter-*download* akan disimpan di dalam *folder binaries*. Kemudian untuk kepentingan lebih lanjut, isi yang ada di dalam *folder binaries* akan di salin ke portal virustotal sehingga bisa dilakukan analisis sederhana *malware*.

4.6.1. Dionaea

Pada penelitian ini versi dionaea yang digunakan adalah 0.8.0. Sebelum melakukan instalasi *dionaea* terlebih dahulu perlu menginstal beberapa *libarary* pendukung. Beberapa *libarary* pendukung yang diperlukan adalah sebagai berikut: *build-essential, cmake, check , cython3 , libcurl4-openssl-dev , libemu-dev, libev-dev, libglib2.0-dev, libloudmouth1-dev, libnetfilter-queue-dev, libnl-3-dev, libpcap-dev, libssl-dev, libtool, libudns-dev, python3, python3-dev, python3-bson, python3-yaml, python3-boto3, ttf-liberation.*

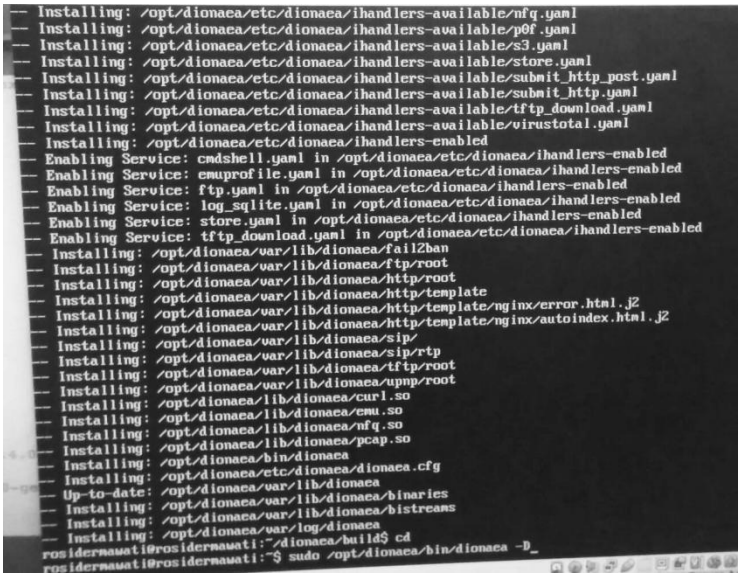
Tahapan selanjutnya melakukan instalasi *libarary* pendukung denga *syntax* yang dapat dilihat dari gambar 4.6.1 di bawah ini:

```
rosidermawati@rosidermawati:~$ sudo apt-get install \
    build-essential \
    cmake \
    check \
    cython3 \
    libcurl4-openssl-dev \
    libemu-dev \
    libev-dev \
    libglib2.0-dev \
    libloudmouth1-dev \
    libnetfilter-queue-dev \
    libnl-3-dev \
    libpcap-dev \
    libssl-dev \
    libtool \
    libudns-dev \
    python3 \
    python3-dev \
    python3-bson \
    python3-yaml \
    python3-boto3 \
    ttf-liberation
```

Gambar 4.6.1. Konfigurasi *Library* Pendukung

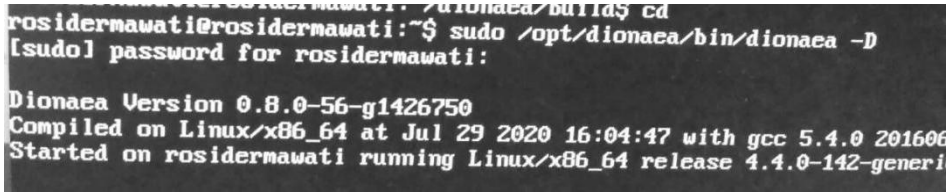
Setelah proses instalasi *library* pendukung berhasil, langkah selanjutnya adalah melakukan *compiling source dionae* ke *github* dengan *syntax*: *git clone* https://github.com/DinoTools/dionaea.git. Setelah berhasil melakukan *clone* langkah selanjutnya masuk ke direktori dionaea dengan *syntax : cd dionaea.* Setelah berada di direktori *dionaea* buatlah sebuah direktori baru dengan

syntax:mkdir build. Masuk ke direktori baru tadi dengan *syntax: cd build.* Setelah berada di direktori *build, run cmake* untuk *setup build process* dengan *syntax: cmake -DCMAKE_INSTALL_PREFIX:PATH=/opt/dionaea ..*, selanjutnya *run make* untuk *build* dan *run make install* untuk menginstal *honeypot.* Hasil yang ditampilkan harus mirip dengan gambar di bawah ini:



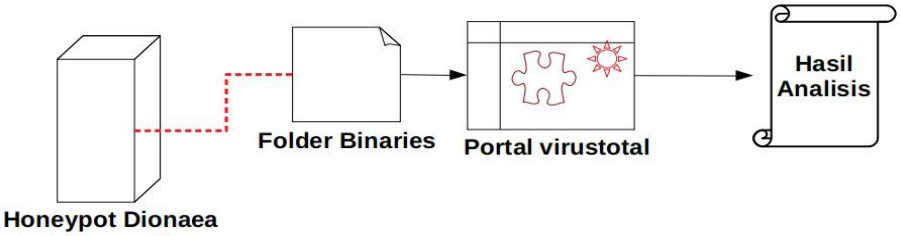
Gambar 4.6.1. Proses Konfigurasi *Honeypot Dionaea*

Setelah semua proses di atas selesai tanpa ada *error,* jalankan *dionaea* dengan *syntax: sudo /opt/dionaea/bin/dionaea -D.*



Gambar 4.6.1. *Dionaea* Berhasil Dijalankan

4.7. Analisis Sederhana *Malware*



Gambar 4.7. Alur Analisis Sederhana *Malware*

Pada gambar 4.7. di atas merupakan alur dari analisis sederhana *malware* dalam penelitian ini. Setelah nantinya *sensor honyepot dionaea* berhasil mendapatkan *sample malware* maka akan dilakukan tahapan analisis dengan memanfaatkan tools *online* viririustotal.com.

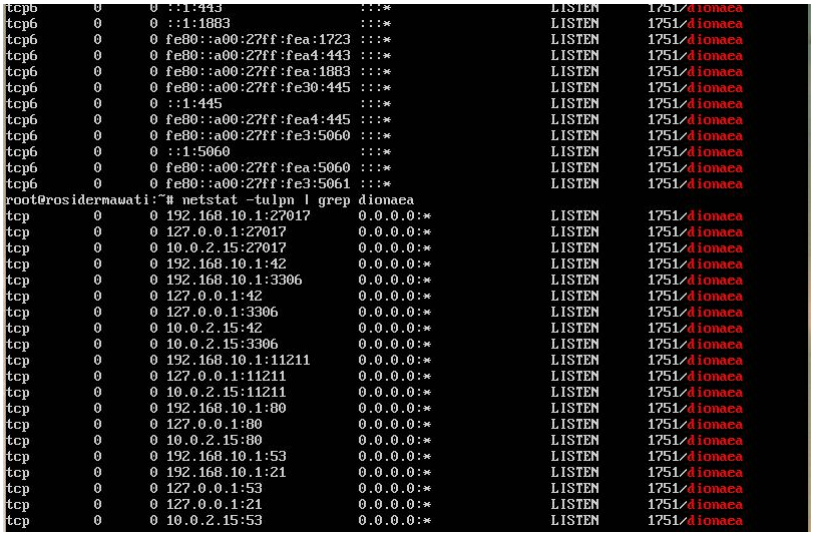
BAB V

HASIL IMPLEMENTASI DAN ANALISIS

5.1. Honeypot Dionaea

Langkah awal yang dapat dilihat menjadi kunci keberhasilan implementasi *honeypot dionaea* dilihat dari pertama kali *honeypot dionaea* dijalankan. Untuk menjalankan *dionaea* dapat menggunakan perintah: /opt/dionae/bin/dionaea –D. Aapabila tidak ada pesan *error* maka *honeypot dionaea* telah terinstal dengan baik.

Langkah selanjutnya memastikan apakah *honeypot dionaea* terlah berjalan dengan benar dapat dilakukan pengecekan terhadap IP dan *port* yang telah *listen* dengan perintah: *netstat –tulpn | grep dionaea.* Perhatikan gambar di bawah ini:



Gambar 5.1. IP dan *Port* yang *Listen*

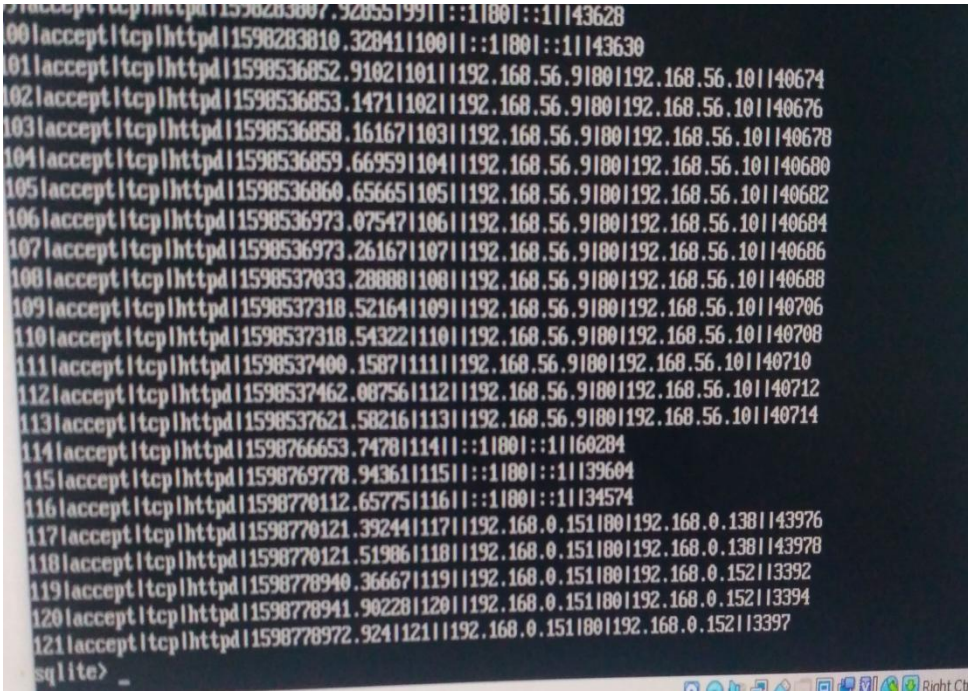
Harus dilakukan validasi dengan cara memastikan port yang terbuka itu diantaranya 445, 21, 3306, 135, 5060, 506, 80. Ini tandanya *port-port* tersebut telah tersedia yang berarti *honeypot dionaea* telah berjalan dengan benar.

Validasi tahap terakhir dapat dilakukan dengan cara melihat secara langsung pada folder: */opt/dionaea/var/lib/dionaea/bistream.* Apabila di dalamnya

terdapat folder dengan format tanggal maka *dionaea* telah berhasil mencatat trafik yang masuk pada tanggal tersebut. Perhatikan gambar di bawah ini:

Gambar 5.1. Isi *Folder Bistreams*

Untuk melihat trafik koneksi yang masuk ke dalam *dionaea* dapat menggunakan perintah *"sqlite3 dionaea.sqlite"* selanjutnya dapat menggunakan perintah pemanggilan tabel yang diinginkan. Contohnya tabel koneksi dengan perintah *"SELECT * FROM connections;"*. Perhatikan gambar di bawah ini:



Gambar 5.1. Koneksi yang Masuk ke *Dionaea*

Pada gambar di atas diambil contoh yang paling terakhir didapatkan keterangan seperti :

121	Id trafik yang berhasil masuk ke dalam sensor *honeypot dionaea*.
Accept	Status yang diterima
Tcp	Protokol yang digunakan
Httpd	Service yang digunakan
1598778972.924	Waktu masuknya trafik dalam bentuk *timestamp*
192.168.0.151	IP target
80	Port yang dimasuki
192.168.0.152	IP penyerang
53940	Port yang digunakan si penyerang untuk masuk

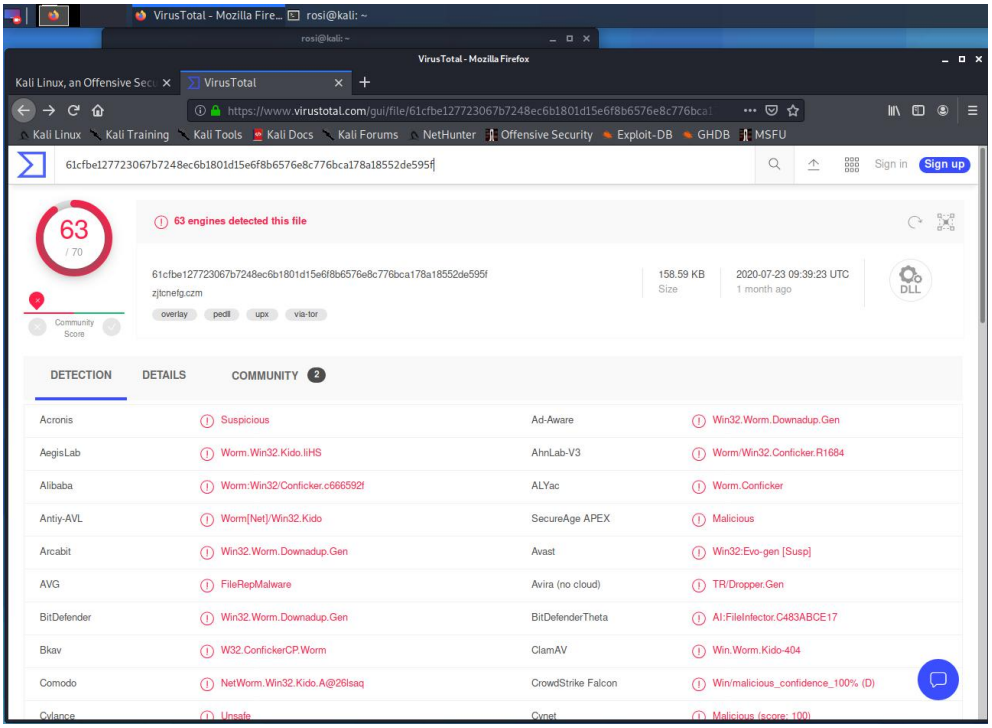
Tabel 5.1. Rincihan Data Koneksi yang Masuk

5.2. Virustotal

Untuk melakukan simulasi analisis sederhana *malware* dapat menggunakan *tools online* seperti virustotal.com. Virustotal menggunakan *hash malware* dalam proses pengidentifikasiannya. Data *malware* yang telah disiapkan dalam bentuk *hash* md5 yaitu: e1855fbe6cf64738bffb9dc195e38ed1, yang dapat dilihat di dalam folder *binaries.* Perhatikan gambar di bawah ini:

```
rosidermawati@rosidermawati:~$ cd /opt/dionaea/var/lib/dionaea/
rosidermawati@rosidermawati:/opt/dionaea/var/lib/dionaea$ ls
binaries  bistreams  dionaea.sqlite  fail2ban  ftp  http  sip  tftp  upnp
rosidermawati@rosidermawati:/opt/dionaea/var/lib/dionaea$ cd binaries
rosidermawati@rosidermawati:/opt/dionaea/var/lib/dionaea/binaries$ ls
e1855fbe6cf65738bffb9dc195e38ed1
rosidermawati@rosidermawati:/opt/dionaea/var/lib/dionaea/binaries$
```

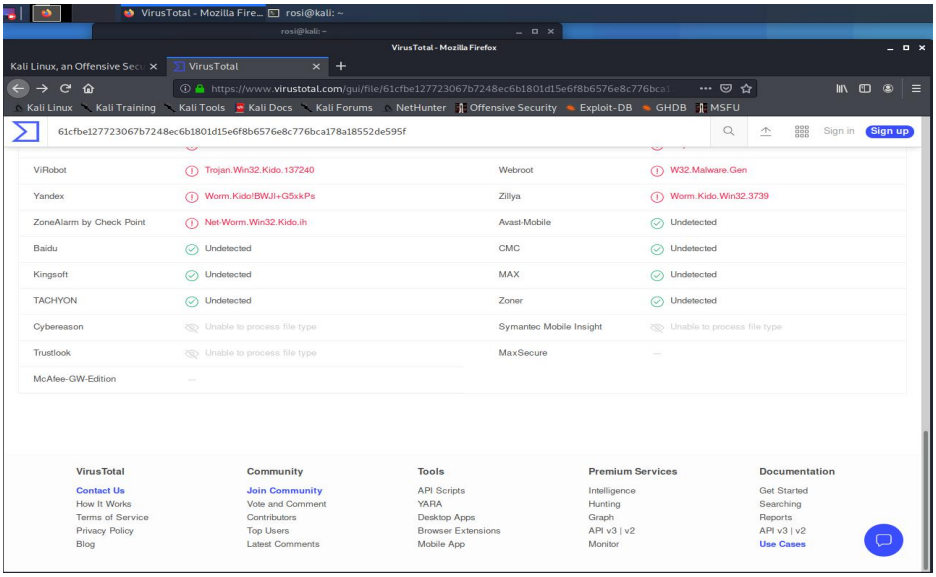
Gambar 5.2. Isi *Folder Binaries.*



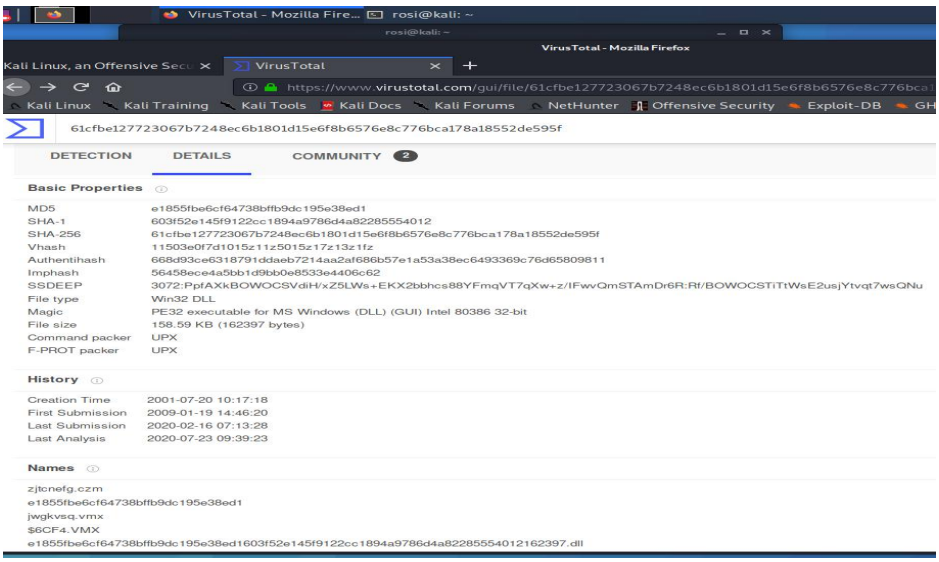
Gambar 5.2. Antivirus yang Bisa Mendeteksi *Malware* di Virustotal

Berdasarkan gambar di atas ada 63 dari 70 jenis antivirus yang bisa mendeteksi *malware* ini. *Malware* ini sejenis *worm*, mempunyai banyak nama tetapi hanya memiliki 1 *hash* md5 yang sama. *Worm* ini lumayan berbahaya karena bisa menggandakan dirinya sendiri serta bisa berjalan tanpa di eksekusi terlebih dahulu. *Malware* jenis ini akan memanfaatkan kerentanan dalam layanan *Microsoft Windows Server* untuk menginfeksi komputer lainnya dalam jaringan.

Gambar di bawah ini merupakan antivirus yang tidak bisa mendeteksi *hash* md5 *malware* yang dimasukkan ke virustotal. Sebaiknya jangan menggunakan antivirus tersebut untuk keamanan komputer.



Gambar 5.2. Antivirus yang Tidak Bisa Mendeteksi *Malware*



Gambar 5.2. *Detail Malware*

BAB VI

KESIMPULAN DAN SARAN

6.1. Kesimpulan

Kesimpulan yang didapatkan dari perlaksaan penelitian tugas akhir ini diantaranya:

1. *Honeypot dionaea* telah berhasil diimplementasikan di jaringan Fakultas Teknik UNIKS. Setelah dijalankan selama 4 minggu telah banyak trafik yang berhasil ditangkap terutama yang melakukan koneksi .
2. Virustotal.com berhasil diimplementasikan sebagai *tools* analisis sederhana *malware.*

6.2. Saran

Saran yang dapat diberikan untuk penelitian selanjutnya dari pelaksanaan tugas akhir ini diantaranya:

1. Memasang sensor *honeypot dionaea* di server asli.
2. Menggunakan jenis *hight interaction honeypot* untuk hasil informasi yang lebih akurat dan terperinci.
3. Menggunakan *tools* analisa *malware* yang berbayar sehingga dapat menghasilkan laporan yang lebih lengkap.

DAFTAR PUSTAKA

[1] P. Studi, T. Informatika, and F. Teknik, "MENGGUNAKAN DIONAEA (Malware Detection in the Network Using Dionaea) Harjono," vol. 14, no. 2, pp. 64–69, 2013.

[2] C. S. Bayu, "Analisis Penerapan Jaringan Keamanan Menggunakan IDS dan Honeypot," *Skripsi, Fak. Ilmu Komput.*, pp. 1–23, 2014.

[3] T. A. Cahyanto, H. Oktavianto, and A. W. Royan, "Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 1, no. 2, pp. 86–92, 2013.

[4] P. Soepomo, "Penerapan Sistem Keamanan Honeypot dan Ids pada Jaringan Nirkabel (Hotspot)," vol. 1, no. 1, pp. 111–118, 2013, doi: 10.12928/jstie.v1i1.2512.

[5] A. F. Nurrahman, "Low-Interaction Honeypot Dengan Dionaea Untuk Mendukung Keamanan Jaringan," vol. 2, no. 4, 2019.

[6] Yuisar, L. Yulianti, and H. Yanolanda Suzantry, "Analisa Pemanfaatan Proxy Server Sebagai Media Filtering Dan Caching Pada Jaringan Komputer," *J. Media Infotama*, vol. 11, no. 1, pp. 81–90, 2015.

[7] F. B. Alfiansyah, "IMPLEMENTASI MONITORING AUTONOMOUS SPREADING MALWARE DI ITS-NET DENGAN DIONAEA DAN CUCKOO," vol. 3, no. 2, pp. 54–67, 2015, [Online]. Available: http://repositorio.unan.edu.ni/2986/1/5624.pdf.

[8] Alamsyah, "Implementasi keamanan instrusion detection system (ids) dan instrusion prevention system (ips) menggunakan clearos," *J. SMARTek, Vol. 9 No. 3*, vol. 9, no. 3, pp. 223–229, 2011.

[9] R. F. Sri Supatmi, Taufiq Nuzwir Nizar, "Perangkat Pendukung Forensik Lalu Lintas Jaringan," *Perangkat Pendukung Forensik Lalu Lintas Jar.*, vol. 3, no. 2, pp. 32–33, 2016, [Online]. Available: https://repository.unikom.ac.id/30336/1/5-perangkatpendukungforensik-aprianti.pdf.

[10] Y. Mardiana and J. Sahputra, "Analisa Performansi Protokol TCP , UDP dan SCTP," *Anal. Performnsi Protoc. TCP, UDP dan SCTP*, vol. 13, no. 2, pp. 73–84, 2017.

[11] Sriyanta, W. W. Winarno, and Sudarmawan, "Optimalisasi Penggunaan

Hardware Server Mempergunakan Virtualisasi Server di SMAN 1 Wonosari," *J. Inf. Politek. Indonusa*, vol. 4, no. 2, pp. 35–42, 2018.

[12] R. Andros and Lukas, "Sebagai Alat Bantu Pendeteksi Keamanan Honeypot Implementation With Pi Raspberry As a Tool for Security Network Detection and," *IMPLEMENTASI HONEYPOT DENGAN RASPBERRY PI SEBAGAI ALAT BANTU PENDETEKSI KEAMANAN Jar. DAN PENANGKAPAN MALWARE*, vol. 4, no. November 2014, pp. 12–26, 2015.

[13] R. Hermawan, "Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)," *Anal. Konsep Dan Cara Kerja Serangan Komput. Distrib. Denial Serv.*, vol. 5, no. 1, pp. 1–14, 2013.