p-ISSN 2407-4489
e-ISSN 2528-7303

IMPLEMENTASI HONEYPOT PADA JARINGAN INTERNET LABOR FAKULTAS TEKNIK UNIKS MENGGUNAKAN DIONAEA SEBAGAI KEAMANAN JARINGAN

Rosi Dermawati[1], M. Hasim Siregar[2]
[1,2]Universitas Islam Kuantan Singingi
Kuantan Singingi, Indonesia
[1]*rosi.dermawati@gmail.com* , [2] *hasyimsiregar92@gmail.com*

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 dengan hanya menggunakan IDS *administrator* jaringan akan kewalahan memeriksa setiap pemberitahuan yang diberikan oleh IDS. IDS inin bekerja hampir sama dengan 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 dirancang untuk menjebak penyerang, 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 cause of computer problems. There are many computers that do not update their antivirus and some even do not use an antivirus. Network security techniques usually block attacks using a firewall or detect attack with IDS (Intruction Detection System), which is in charge of guarding against axisting 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, additional security is needed such as a dionaea honeypot. A honeypot is a fake system the signed to trap attacker, as if it were a real system. Based on these problems, a research will be conducted on the Analysis And Implementation Of Honeypot Using Dionaea as Network Security Support.

Keywords: Honeypot, Dionaea, IDS, Firewall, Malware

PENDAHULUAN

Sistem komputer menjadi bagian yang sangat penting dan tidak dapat dipisahkan dalam dunia pendidikan. *Internet* merupakan jaringan komputer yang bersifat publik. Malware (Malicious Software) merupakan sebuah program yang dirancang dengan tujuan untuk masuk menyusup ke sebuah sistem komputer, yang akan merusak sistem komputer tersebut. Malware dapat masuk ke banyak komputer melalui jaringan internet seperti email, download dari internet, atau melalui program yang terinfeksi (Tedyyana & Supria, 2018). *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. Menurut (Sutarti et al., 2018) *Intrusion Detection System* (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Namun IDS sendiri tidak serta merta dapat menahan serangan para penyerang. Selain menggunakan cara konvensional tersebut pengamanan sistem jaringan dapat menggunakan *honeypot*. *Honeypot* dapat mengalihkan penyerang dengan seolah-olah menjadi server asli sehingga dapat menjadi tempat untuk berinteraksi sementara bagi penyerang yang ingin melakukan serangan (Agustino et al., 2017). implementasi honeypot low interaction memanfaatkan dua aplikasi yang berbeda, yaitu Dionaea dan Honeyd berhasil membuat layanan palsu sebagai target serangan dan mencatat aktivitas yang dianggap dapat membahayakan sistem dan jaringan, namun tidak adanya interaksi lebih lanjut ketika penyerang berhasil mengeksploitasi dan masuk dalam honeypot (Arkaan & Sakti, 2019). Sehingga seorang *administrator* jaringan dapat melihat dengan nyata informasi suatu serangan yang terjadi pada layanan. *Honeypot* ini sangat penting untuk menjadi suatu perangkat tambahan demi meminimalisir serangan yang terjadi ke dalam sistem.

Menurut (Cahyanto, TA; Oktavianto, H; Royan, 2017)

dionaea adalah honeypot yang bersifat *Low Interaction Honeypot* yang diciptakan sebagai pengganti *Nepenthes, dionaea* menggunakan bahasa pemrograman *python* sebagai bahasa *scripting, libemu* untuk mendeteksi *shellcode,* mendukung *Ipv6* dan *TLS. Dionaea* bertujuan untuk mendapatkan duplikasi data dari *malware. 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".

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah: Berhasil mengimplementasikan *honeypot dionaea* di salah satu komputer labor. Penganalisaan serangan atau *malware* yang dilakukan oleh seorang *administrator* jaringan dengan *honeypot dionaea* menjadi lebih terorganisir dan tepat sasaran.

Dengan melakukan penelitian ini diharapkan bisa memberikan manfaat antara lain: Dengan menerapkan *honeypot dionaea* sebagai teknik keamanan jaringan dapat membantu *administrator* jaringan mengetahui perilaku *malware.* Informasi data *malware* dapat digunakan oleh *administrator* jaringan untuk mempelajari perilaku *malware* serta pencegahan yang dapat dilakukan.

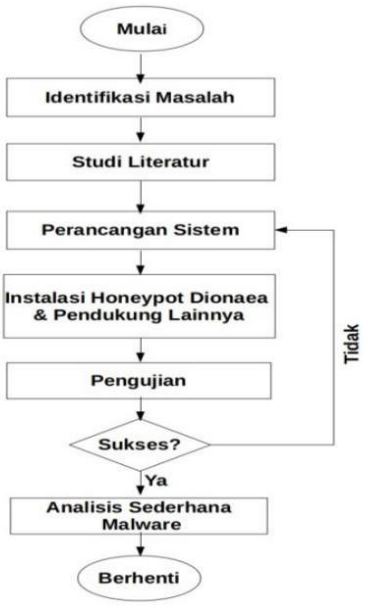
METODE PENELITIAN

Teknik pengumpulan data dan informasi yang penulis gunakan dalam penelitian ini adalah sebagai berikut seperti pada Gambar 1:

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.

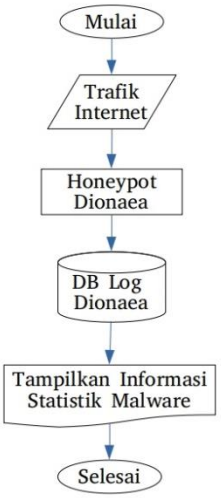


Gambar 1. Diagram alur penelitian

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.

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.



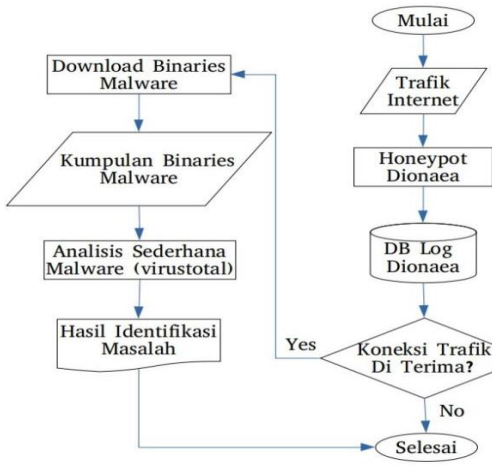
Gambar 2. *Flowchart* cara kerja sistem *honeypot dionaea* dan virus total

Pada Gambar 2 menunjukkan *flowchart* cara kerja sistem *honeypot dionaea* dan 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.*
4. Setiap trafik jaringan internet yang masuk akan dicek, Apabila statusnya ditolak maka proses akan berhenti. Apabila statusnya diterima, *dionaea* akan melanjutkan proses *download binaries malware.*
5. *Folder binaries* akan menyimpan data *binaries malware* yang telah berhasil ter-

download.

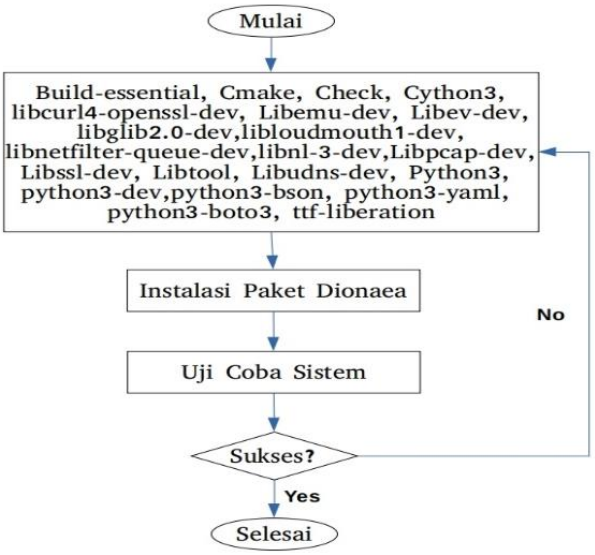
6. Data *binaries malware* akan diproses menggunakan portal virustotal untuk dilakukan identifikasi jenis dan perilaku *malware.*
7. Dari analisis sederhana menggunakan virustotal akan menghasilkan laporan yang menunjukkan jenis dan perilaku *malware*



Gambar 3. Cara kerja *honeypot dionaea*

Pada Gambar 3 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.*



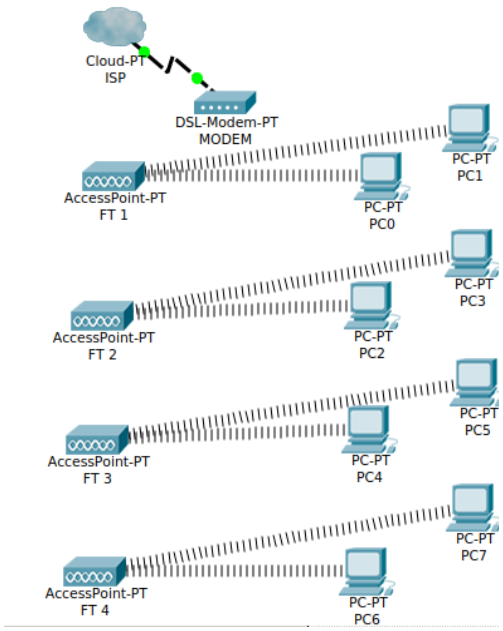
Gambar 4. Tahap konfigurasi honeypot dionaea

Pada Gambar 4 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.



Gambar 5. Topologi jaringan

Gambar 5 menunjukkan Topologi Jaringan yang digunakan pada penelitian ini. *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.

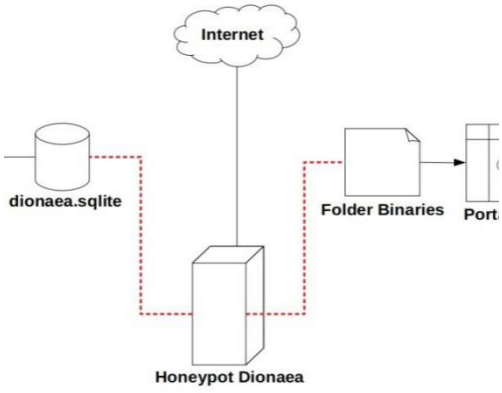
Honeypot Dionaea akan diinstal di sebuah komputer dengan spesifikasi sebagai berikut:

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.

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/bin

aries". Selanjutnya isi didalam *folder binaries* akan disalin ke portal virustotal untuk dilakukan penganalisaan.



Gambar 6. Pembangunan sistem

Berdasarkan Gambar 6, 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*.

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 seperti Gambar 7 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
```

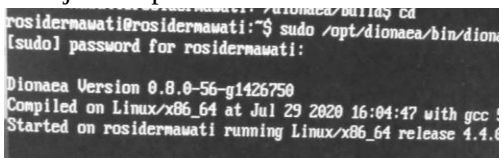
Gambar 7. Library pendukung dionaea

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*](https://github.com/DinoTools/dionaea.git).

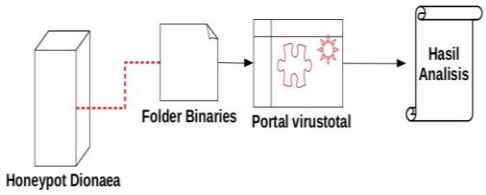
Setelah berhasil melakukan *clone* langkah selanjutnya masuk ke direktori dionaea dengan *syntax : cd dionaea*. Setelah berada di direktori *dionaea* buatlah sebuah direktori baru dengan *syntax:mkdir build*. Masuk ke direktori baru tadi dengan *syntax: cd build*. Setelah berada di direktori *build, 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 8.

Gambar 8. Proses konfigurasi *honeypot dionaea*

Setelah semua proses di atas selesai tanpa ada *error*, jalankan *dionaea* dengan *syntax: sudo /opt/dionaea/bin/dionaea –D* yang ditunjukkan pada Gambar 9.



Gambar 9. Dionaea berhasil dijalankan



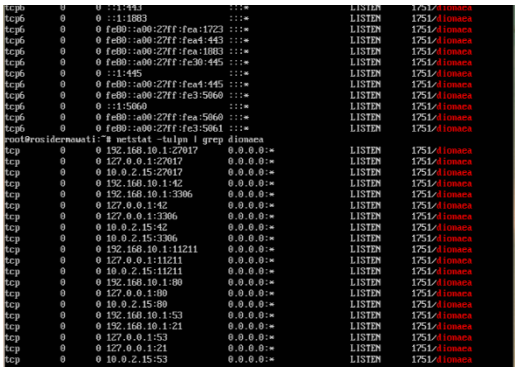
Gambar 10. Alur analisis sederhana *malware*

Pada Gambar 10 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* virirustotal.com.

HASIL PENELITIAN DAN PEMBAHASAN

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 11 di bawah ini:



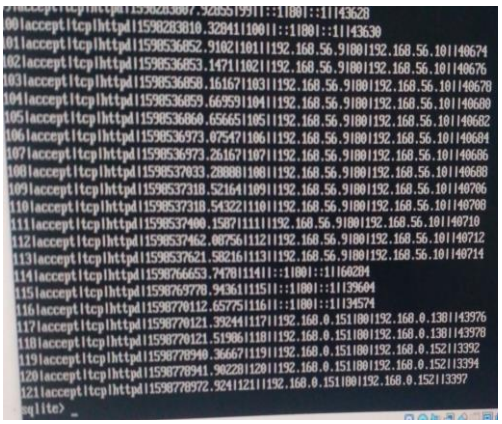
Gambar 11. IP dan port yang *listen*

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/bistrea m.* Apabila di dalamnya terdapat folder dengan format tanggal maka *dionaea* telah berhasil mencatat trafik yang masuk pada tanggal tersebut. Perhatikan Gambar 12 di bawah ini:

Gambar 12. 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 13 di bawah ini:

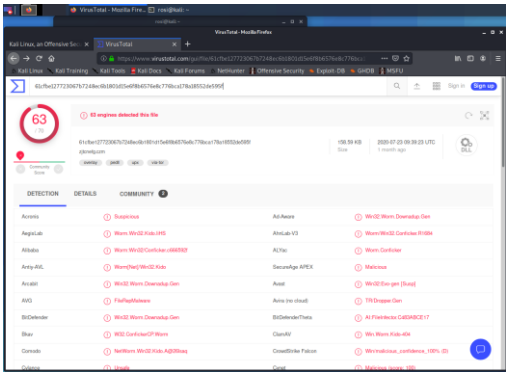


Gambar 13. Koneksi yang masuk ke *dionaea*

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 14 di bawah ini:

Gambar 14. Isi *folder binaries*

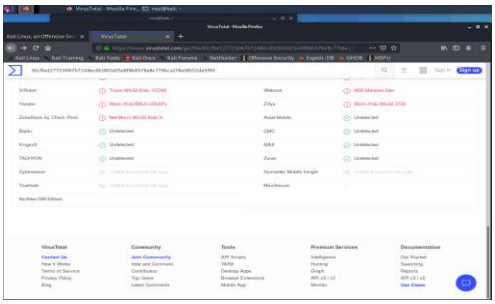


Gambar 15. Antivirus yang bisa mendeteksi *malware* di virustotal

Berdasarkan Gambar 15, 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

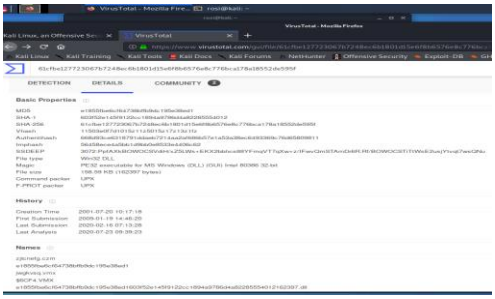
layanan *Microsoft Windows Server* untuk menginfeksi komputer lainnya dalam jaringan.

Gambar 16 menunjukkan antivirus yang tidak bisa mendeteksi *hash* md5 *malware* yang dimasukkan ke virustotal. Sebaiknya jangan menggunakan antivirus tersebut untuk keamanan komputer.



Gambar 16. Tidak bisa mendeteksi *malware*

Gambar 17 menunjukkan detail malware yang berhasil didapatkan oleh *honeypot dionaea.*



Gambar 17. *Detail Malware*

KESIMPULAN DAN SARAN

Kesimpulan yang didapatkan dari perlaksaan penelitian 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 dengan server.

2. Virustotal.com berhasil diimplementasikan sebagai *tools* menganalisis sederhana *malware* yang telah didapatkan dari hasil H*oneypot dionaea.*

Saran yang dapat diberikan untuk penelitian selanjutnya dari penelitian ini diantaranya:

1. Menggunakan jenis *hight interaction honeypot* untuk hasil informasi yang lebih akurat dan terperinci.
2. Menggunakan *tools* analisa *malware* yang berbayar sehingga dapat menghasilkan laporan yang lebih lengkap.

DAFTAR PUSTAKA

Agustino, D. P., Priyoatmojo, Y., & Safitri, N. W. W. (2017). Implementasi Honeypot Sebagai Pendeteksi Serangan dan Melindungi Layanan Cloud Computing. *Konferensi Nasional Sistem & Informatika 2017*, 196–201.

Arkaan, N., & Sakti, D. V. S. Y. (2019). Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH. *Jurnal Nasional Teknologi Dan Sistem Informasi*, *5*(2), 112–120. https://doi.org/10.25077/teknosi.v5i2.2019.112-120

Cahyanto, TA; Oktavianto, H; Royan,

A. (2017). Analisis Dan Implementasi Honeypot Menggunakan Donaea Sebagai Penunjang Keamanan Jaringan. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Sutarti, Pancaro, Adi, P., & Saputra, Fembi, I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, *5*(1), 1–8. http://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/download/584/592

Tedyyana, A., & Supria, S. (2018). Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway. *INOVTEK Polbeng - Seri Informatika*, *3*(1), 34. https://doi.org/10.35314/isi.v3i1.340