PERANCANGAN INFRASTRUKTUR LABORATORIUM MALWARE DI PROGRAM STUDI TEKNIK INFORMATIKA UNIVERSITAS PASUNDAN BANDUNG

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1,
Program Studi Teknik Informatika, Universitas Pasundan Bandung

oleh :

Yuana Kania Madya
NRP : 13.304.0067

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
DESEMBER 2017

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berta acara sidang, tugas akhir dari :

Nama : Yuana Kania Madya
Nrp : 13.304.0067

Dengan judul :

"**PERANCANGAN INFRASTRUKTUR LABORATORIUM MALWARE DI PROGRAM STUDI TEKNIK INFORMATIKA UNIVERSITAS PASUNDAN BANDUNG**"

Bandung, 28 Desember 2017

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
(Doddy Ferdiansyah, S.T, M.T)	(Ferry Mulyanto, S.T, M.Kom.)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas akhir ini adalah benar-benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya
2. Tugas akhir ini merupakan gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing
3. Dalam tugas akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian-bagian tertentu dalam penulisan laporan Tugas Akhir yang saya kutip dari hasil karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab saya, bukan tanggung jawab Universitas Pasundan Bandung

Apabila di kemudian hari ditemukan seluruh atau sebagian laporan tugas akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian-bagian tertentu, saya bersedia menerima sangsi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya

.

Bandung, 28 Desember 2017

Yang membuat pernyataan,

Materai
6000,-

(Yuana Kania Madya)

NRP. 13.304.0067

ABSTRAK

Malware merupakan program komputer yang dirancang khusus untuk melakukan aktifitas yang tidak diinginkan oleh pemiliknya atau mengganggu sebuah sistem komputer bahkan bisa merusaknya. Memahami *malware* beroperasi bisa dijadikan sebuah pembelajaran bagi mahasiswa yaitu untuk lebih dalam menganalisis *malware*. Permasalahannya adalah mahasiswa mungkin akan merasa takut ketika mereka akan menganalisis *malware* di laptop atau komputer mereka masing-masing karena kemungkinan *malware* akan tersebar kedalam sistem komputer atau laptop dari mahasiswa tersebut. Oleh sebab itu harus disediakannya fasilitas khusus yang digunakan untuk mahasiswa dalam mengekplorasi *malware* agar mencegah *malware* yang sedang dianalisis tidak menyerang sistem komputer kita. Fasilitas yang dibutuhkan yaitu menyerupai sebuah laboratorium yang khusus digunakan untuk eksplorasi dan pembelajaran lebih dalam mengenai *malware*.

Penelitian ini dimulai dari identifikasi masalah kemudian melakukan pengumpulan data dengan cara wawancara dan observasi ditempat penelitian. Hal pertama yang dilakukan yaitu observasi infrastruktur jaringan apa saja yang ada di tempat penelitian. Perancangan lab *malware* berdasarkan spesifikasi dari perangkat jaringan yang ada di tempat penelitian.

Hasil dari perancangan ini akan menggunakan tool analisis *malware* yaitu *cuckoo sandbox* yang dapat memberikan informasi dari hasil analisis statis dan analisis dinamis. Proses yang dilakukan oleh *cuckoo sandbox* yaitu akan membuat lingkungan yang terisolasi di dalam sebuah *virtual machine* dengan menggunakan sebuah *virtual networking* yaitu *host-only networking* dan ketika terjadi kerusakan pada *virtual machine* tidak akan berpengaruh kepada *host* dan mengatasi hal itu hanya tinggal menginstall ulang kembali *virtual machine*.

Kata Kunci : Malware, Analisis Malware, Lab Malware, Sandbox, Cuckoo Sandbox

ABSTRACT

Malware is a computer program designed specifically to perform activities that are not desired by the owner or interfere with a computer system can even damage it. Understanding operating malware can be used as a learning for students is to more deeply analyze malware. The problem is that students may be afraid when they will analyze the malware on their laptop or computer because of the possibility of malware will be spread into the computer system or laptop of the student. Therefore must provide special facilities used for students in exploring malware in order to prevent malware being analyzed does not attack our computer system. The facilities needed are like a laboratory specifically used for exploration and deeper learning about malware.

This research starts from the identification problem then do the data collecting by interview and observation in the place of research. the first thing to do is observation of any network infrastructure that is in place of research. The design of malware labs based on the specifications of the existing network devices in place of research.

The results of this design will use a malware analysis tool that is cuckoo sandbox that can provide information from the results of static analysis and dynamic analysis. The process done by cuckoo sandbox is to create an isolated environment inside a virtual machine using a virtual networking that is host-only networking and when there is damage to the virtual machine will not affect the host and overcome it just to re-install the virtual machine.

Keyword : Malware, Analisis Malware, Lab Malware, Sandbox, Cuckoo Sandbox

KATA PENGANTAR

Ucapan dan rasa syukur penulis layangkan ke hadirat Ilahi Robbi, yang telah berkenan menguatkan penulis untuk membuat Laporan Tugas Akhir dengan judul "Analisis Sistem Informasi Eksekutif untuk Perguruan Tinggi (Studi Kasus Universitas Pasundan)".

Adapun penulisan laporan ini bertujuan untuk memenuhi salah satu syarat kelulusan Program Strata 1, di Program Studi Teknik Informatika Universitas Pasundan.

Penulis menyadari laporan ini dapat terwujud berkat bantuan dan dorongan dari berbagai pihak. Maka pada kesempatan ini penulis sampaikan terima kasih yang sebesar-besarnya atas segala bantuan yang penulis terima baik secara moril maupun materil, sehingga penulis dapat menyelesaikan laporan ini kepada :

1. Pembimbing Utama, Bapak Doddy Ferdiansyah, S.T, M.T
2. Pembimbing Pendamping, Bapak Ferry Mulyanto, S.T, M.Kom.
3. Kepada Orang Tua tersayang, dan keluarga yang selalu memberikan motivasi serta do'anya dalam pembuatan tugas akhir ini.
4. Koordinator Tugas Akhir dan Ketua Kelompok Keilmuan serta seluruh civitas akademika Teknik Informatika di UNIVERSITAS PASUNDAN BANDUNG, yang telah memberikan bekal ilmu selama penulis menimba ilmu.
5. Kepada teman-teman seperjuangan Universitas Pasundan Bandung yang tidak bisa semua penulis sebutkan.

Tiada gading yang tak retak, tiada gelombang tanpa ombak, segala kesalahan merupakan kelemahan dan kekurangan penulis. oleh karena itu, penulis harapkan kritik dan saran dari semua pihak demi perbaikan di masa yang akan datang.

Akhir kata, semoga penulisan laporan ini dapat bermanfaat bagi penulis dan bagi perkembangan ilmu Teknologi dimasa yang akan datang.

Bandung, 28 Desember 2017

Penulis

DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI iv
DAFTAR ISTILAH viii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR LAMPIRAN xiii
BAB I PENDAHULUAN 1-1
1.1 Latar Belakang 1-1
1.2 Identifikasi Masalah 1-1
1.3 Tujuan Tugas Akhir 1-2
1.4 Lingkup Tugas Akhir 1-2
1.5 Metodologi Pengerjaan Tugas Akhir 1-2
1.6 Sistematika Penulisan Tugas Akhir 1-3
BAB 2 LANDASAN TEORI 2-1
2.1 *IT Infrastructure* 2-1
2.1.1 *Infrastructure Building Block* 2-2
2.2 Laboratorium 2-3
2.3 *Malware* 2-3
2.3.1 *History Of Malware* 2-3
2.3.2 Jenis-jenis *Malware* Menurut Gov-CSIRT 2-4
2.3.2.1 *Virus* 2-4
2.3.2.2 *Trojan Horse* 2-5
2.3.2.3 *Worm* 2-5
2.3.2.4 *Trapdoor* 2-6
2.3.2.5 *Logic Bomb* 2-6
2.3.2.6 *Spyware* 2-6
2.3.2.7 *Rootkit* 2-7
2.3.2.8 *Bot and Botnet* 2-8
2.3.2.9 *Adware* 2-8
2.3.2.10 *Bug* 2-9
2.3.2.11 *Ransomware* 2-9
2.3.3 Analisis *Malware* 2-11
2.3.3.1 Teknik Analisis *Malware* 2-11
2.3.3.2 *Tools* Analisis *Malware* 2-12

2.3.3.3 Lab *Malware* 2-12
2.4 Jaringan Komputer 2-12
2.4.1 Klasifikasi Jaringan Komputer 2-12
2.4.1.1 Jenis Jaringan Komputer Berdasarkan Skala atau Area 2-13
2.4.1.2 Jenis Jaringan Komputer Berdasarkan Media Penghantar 2-14
2.4.1.3 Jenis Jaringan Komputer Berdasarkan Pola Operasi 2-15
2.4.2 Topologi Jaringan 2-15
2.4.2.1 Topologi Jaringan *Bus* 2-16
2.4.2.2 Topologi Jaringan *Star* 2-17
2.4.2.3 Topologi Jaringan *Ring* 2-18
2.4.2.4 Topologi Jaringan *Tree* 2-19
2.4.2.5 Topologi Jaringan *Mesh* 2-19
2.4.3 Perangkat Jaringan 2-20
2.4.3.1 *Switch* 2-20
2.4.3.2 Kabel 2-21
2.4.3.3 *Router* 2-23
2.5 *Sandbox* 2-24
2.5.1 *Cuckoo Sandbox* 2-24
2.5.2 *Architecture Cuckoo Sandbox* 2-25
2.6 Diagram Sebab dan Akibat *(Cause and Effect Diagram)* 2-26
2.6.1 Karakteristik Diagram Sebab dan Akibat 2-26
2.6.2 Keuntungan Diagram Sebab dan Akibat 2-27
2.6 Penelitian Terdahulu 2-24
BAB 3 SKEMA PENELITIAN 3-1
3.1 Alur Penelitian 3-1
3.2 Analisis Masalah dan Solusi Tugas Akhir 3-3
3.2.1 Rencana Analisis 3-4
3.2.2 Analisis Solusi IT 3-5
2.2.2.1 *Fishbone Diagram* 3-6
3.3 Kerangka Berfikir Teoritis 3-7
3.4 Profile Objek dan Tempat Penelitian 3-7
3.5 Analisis Masalah Tugas Akhir 3-8
3.5.1 Analisis Konsep 3-9
BAB 4 ANALISIS DAN PERANCANGAN 4-1
4.1 Analisis Keadaan Saat Ini 4-1
4.1.1 Wawancara dengan Pengelola Lab 603 4-1
4.1.1.1 Proses Bisnis 4-1

4.1.2 Infrastruktur Jaringan yang digunakan 4-1
4.1.2.1 Observasi Infrastruktur Jaringan Lab 603 4-2
4.1.2.2 Komponen Infrastruktur Jaringan Lab 603 4-2
4.1.3 Topologi Jaringan Lab 603 4-3
4.1.4 Spesifikasi Infrastruktur Jaringan yang digunakan 4-4
4.1.4.1 Spesifikasi Komputer Lab 603 4-4
4.1.4.2 Spesifikasi *Switch* Lab 603 4-10
4.1.4.3 Kabel Cat 5 4-10
4.2 Analisis Kebutuhan Lab *Malware* 4-10
4.2.1 Teknik Analisis Malware 4-11
4.2.2 Tool Analisis Malware 4-11
4.2.3 *Host OS* 4-13
4.2.4 *Virtualization Software* 4-13
4.2.5 *Guest OS* 4-13
4.3 Perancangan Lab *Malware* 4-14
4.3.1 *Installing Host* 4-14
4.3.2 *Installing Requirement* 4-14
4.3.2.1 *Installing Python Libraries* 4-14
4.3.2.1.1 *Installing Cuckoo Sandbox* 4-14
4.3.2.2 *Installing Virtualization Software* 4-14
4.3.2.3 *Installing Django Web Interface* 4-14
4.3.2.4 *Installing TCPdump* 4-14
4.3.2.5 *Installing Volatility* 4-15
4.3.2.6 *Installing Volatility Plug-ins* 4-15
4.3.2.7 *Installing Mitmproxy* 4-15
4.3.3 *Configuration Cuckoo Sandbox* 4-15
4.3.4 *Guest Operating System Configuration* 4-17
4.3.4.1 *Windows Setting* 4-17
4.3.4.2 *Setting up a Shared Folder* 4-17
4.3.4.3 *Cuckoo Dependencies* 4-18
4.3.4.4 *Network Configuration* 4-18
4.3.5 *Requirement System* 4-18
4.3.6 Topologi Logika *Cuckoo Sandbox* 4-20
4.3.6.1 *Cuckoo Host* 4-19
4.3.6.2 *Virtual Network* 4-21
4.3.6.3 *Cuckoo Guest* 4-21
4.3.7 Rancangan Lab *Malware* 4-22

4.3.8 Topologi Fisik 4-24
4.3.9 *IT Infrastructure Lab Malware* 4-25
BAB 5 KESIMPULAN DAN SARA 5-1
5.1 Kesimpulan 5-1
5.2 Saran 5-1
DAFTAR PUSTAKA

DAFTAR ISTILAH

NO	Daftar Istilah	Pengertian
1	Malware	Malware merupakan singkatan dari Malicious Software, malware diciptakan oleh penyerang untuk kepentingan mereka sendiri, diantaranya untuk menggangu operasi komputer, mencuri informasi atau mendapatkan akses ke dalam sistem.
2	Analisis Malware	Analisis malware adalah seni membedah malware untuk memahami bagaimana cara kerjanya, bagaimana cara mengidentifikasinya, dan bagaimana cara mengalahkan dan menghilangkannya.
3	Lab Malware	Lab Malware adalah sebuah lingkungan yang aman untuk menganalisis malware. Pada dasarnya, lab malware merupakan lingkungan yang terisolasi dan juga sudah terinstal tools yang diperlukan untuk kegiatan analisis yang dapat digunakan untuk membantu dalam menganalisis malware.
4	Sandboxing	Sandboxing juga yang bertujuan menjalankan aplikasi dan file yang tidak diketahui dan tidak terpercaya di dalam lingkungan yang terisolasi dan mendapatkan informasi tentang apa yang dilakukannya.
5	Cuckoo Sandbox	Cuckoo sandbox merupakan Malware Tools Analysis Sistem. Cuckoo Sandbox ini digunakan untuk mengalisis malware, Cuckoo dapat memberikan beberapa informasi mengenai malware yang sedang berjalan dalam lingkungan yang terisolasi
6	Cuckoo Host	Sebuah komputer yang mengelola Guest OS untuk berjalannya analisis
7	Cuckoo Guest	Lingkungan yang terisolasi saat menjalankan malware dan perilaku malware di laporkan kembali ke Cuckoo Host
8	Virtual Network	Sebuah jaringan yang terisolasi dimana kita menjalan kan analisis pada virtual machine
9	Host-only Networking	Host-only networking menyediakan sebuah koneksi jaringan antara virtual machine dan komputer host. Dalam mode ini guest OS dapat mengakses host OS dan sebaliknya host OS juga dapat mengakes guest OS. Host OS dan Guest yang menggunakan mode jaringan host-only adapter secaralangsung mereka berdua akan berada dalam satu jaringan yang sama

DAFTAR TABEL

Tabel 2.1. Jaringan Komputer Berdasarkan Area 2-14
Tabel 2.2. Penelitian Terdahulu 2-28
Tabel 3.1. Rancangan Penelitian Tugas Akhir 3-1
Tabel 3.2. Analisis Masalah dan Solusi 3-3
Tabel 3.3. Langkah Analisis 3-5
Tabel 3.4. Peta Konsep 3-9
Tabel 4.1. Infrastruktur Jaringan Laboratorium TIF 603 4-2
Tabel 4.2. Spesifikasi Komputer 1 4-4
Tabel 4.3. Spesifikasi Komputer 2 4-4
Tabel 4.4. Spesifikasi Komputer 3 4-4
Tabel 4.5. Spesifikasi Komputer 4 4-5
Tabel 4.6. Spesifikasi Komputer 5 4-5
Tabel 4.7. Spesifikasi Komputer 6 4-5
Tabel 4.8. Spesifikasi Komputer 7 4-5
Tabel 4.9. Spesifikasi Komputer 8 4-5
Tabel 4.10. Spesifikasi Komputer 9 4-6
Tabel 4.11. Spesifikasi Komputer 10 4-6
Tabel 4.12. Spesifikasi Komputer 11 4-6
Tabel 4.13. Spesifikasi Komputer 12 4-6
Tabel 4.14. Spesifikasi Komputer 13 4-7
Tabel 4.15. Spesifikasi Komputer 14 4-7
Tabel 4.16. Spesifikasi Komputer 15 4-7
Tabel 4.17. Spesifikasi Komputer 16 4-7
Tabel 4.18. Spesifikasi Komputer 17 4-8
Tabel 4.19. Spesifikasi Komputer 18 4-8
Tabel 4.20. Spesifikasi Komputer 19 4-8
Tabel 4.21. Spesifikasi Komputer 20 4-8
Tabel 4.22. Spesifikasi Komputer 21 4-9
Tabel 4.23. Spesifikasi Komputer Pertama 4-9
Tabel 4.24. Spesifikasi Komputer Kedua 4-9
Tabel 4.25. Spesifikasi Komputer Ketiga 4-10
Tabel 4.26. Spesifikasi Komputer Pertama 4-19
Tabel 4.27. Spesifikasi Komputer Kedua 4-19
Tabel 4.28. Spesifikasi Komputer Ketiga 4-19

DAFTAR GAMBAR

Gambar 1.1. Metodologi Tugas Akhir 1-2
Gambar 2.1. *Infrastructrue Building Block* [LAA13] 2-2
Gambar 2.2. Perangkat yang dapat terinfeksi *Ransomware* [HAG16] 2-9
Gambar 2.3. Contoh dari Layar *Locker Ransomware* [DEL16] 2-10
Gambar 2.4. *How Crypto Ransomware Works* [DEL16] 2-11
Gambar 2.5. Topologi Jaringan *Bus* [ZAK17] 2-16
Gambar 2.6. Topologi Jaringan *Star* [ZAK17] 2-17
Gambar 2.7. Topologi Jaringan *Ring* [ZAK17] 2-18
Gambar 2.8. Topologi Jaringan *Tree* [ZAK17] 2-19
Gambar 2.9. Topologi Jaringan *Mesh* [ZAK17] 2-20
Gambar 2.10. *Switch* [MIC12] 2-21
Gambar 2.11. Kabel UTP [MIC12] 2-21
Gambar 2.12. Kabel FTP [MIC12] 2-22
Gambar 2.13. Kabel STP [MIC12] 2-22
Gambar 2.14. Kabel *Coaxial* [MIC12] 2-23
Gambar 2.15. Kabel *Fiber Optic* [MIC12] 2-23
Gambar 2.16. *Router* [MIC12] 2-23
Gambar 2.17. Arsitektur *Cuckoo Sandbox* [OKT13] 2-25
Gambar 2.18. Diagram Sebab Akibat [KEL95] 2-27
Gambar 3.1. Rencana Analisis 3-4
Gambar 3.2. *Fishbone Diagram* 3-6
Gambar 3.3. Kerangka Pemikiran Teoritis 3-7
Gambar 3.4. *Infrastructrue Building Blocks* 3-8
Gambar 4.1. Topologi Fisik Lab 603 4-3
Gambar 4.2. Analisis Kebutuhan Lab *Malware* 4-11
Gambar 4.3. *Shared Folder* 4-17
Gambar 4.4. Topologi Logika 4-20
Gambar 4.5. Rancangan Lab *Malware* 4-22
Gambar 4.6. Topologi Fisik Lab *Malware* 4-24
Gambar 4.7. IT Infrastruktur Lab *Malware* 4-25
Gambar A.1. Instalasi *The Dependencies* A-1
Gambar A.2. Instalasi libxml2-dev and libxslt-dev A-1
Gambar A.3. *Download* Cuckoo *Sandbox* A-2
Gambar B.1. Instalasi *Virtualization Software* B-1
Gambar B.2. *Website Virtualbox* B-1
Gambar B.3. *Configuration File* B-2

Gambar B.4. Membuka Virtualbox B-2
Gambar B.5. *Create Virtual Machine* B-2
Gambar B.6. *Setting up Memory Size* B-3
Gambar B.7. *Hard Disk File Type* B-3
Gambar B.8. *Storage On Physical Hard Disk* B-4
Gambar B.9. *File Location and Size* B-4
Gambar B.10. Mencari *File ISO* Sistem Operasi B-5
Gambar C.1. Instalasi Django-based Web Interface C-1
Gambar D.1. Instalasi TCPDump D-1
Gambar E.1. Instalasi Volatility *Command* 1 ..... E-1
Gambar E.2. Instalasi Volatility *Command* 2 ..... E-1
Gambar E.3. Instalasi Volatility *Command* 3 ..... E-2
Gambar E.1. Instalasi Volatility *Command* 1 ..... E-1
Gambar E.2. Instalasi Volatility *Command* 2 ..... E-1
Gambar E.3. *Download Distorm 3* E-2
Gambar F.1. Instalasi Volatility *Command* 1 ..... F-1
Gambar F.2. Instalasi Distorm 3 *Command* 1 ..... F-1
Gambar F.3. Instalasi Distorm 3 *Command* 2 ..... F-2
Gambar F.4. Instalasi Distorm 3 *Command* 3 ..... F-2
Gambar F.5. Instalasi autoreconfig F-3
Gambar F.6. Instalasi libtool-bin F-3
Gambar F.7. Ekstrak yara-3.5.0.tar.gz F-4
Gambar F.8. Instalasi Yara *Command* 1 ..... F-4
Gambar F.9. Instalasi Yara *Command* 2 ..... F-5
Gambar F.10. Instalasi Yara *Command* 3 ..... F-5
Gambar F.11. Ekstrak PyCrypto F-6
Gambar F.12. Instalasi Volatility *Command* 2 ..... F-6
Gambar F.13. Instalasi Volatility *Command* 3 ..... F-6
Gambar F.14. Instalasi PyCrypto *Command* 2 ..... F-7
Gambar F.15. Instalasi PyCrypto *Command* 3 ..... F-8
Gambar F.16. Instalasi Openpyxl F-8
Gambar G.1. Instalasi Mitmproxy *Command* 1 ..... G-1
Gambar G.2. instalasi Mitmproxy *Command* 2 ..... G-1
Gambar G.3. Instalasi Mitmproxy *Command* 3 ..... G-2
Gambar H.1. Konfigurasi *File Cuckoo* H-1
Gambar H.2. Konfigurasi cuckoo.conf langkah 1 ..... H-2
Gambar H.3. Konfigurasi cuckoo.conf Langkah 2 ..... H-2

Gambar H.4. Konfigurasi auxiliary.conf H-3
Gambar H.5. Konfigurasi virtualbox.conf Langkah 1 ..... H-4
Gambar H.6. Konfigurasi virtualbox.conf Langkah 2 ..... H-4
Gambar H.7. Konfigurasi virtualbox.conf Langkah 3 ..... H-5
Gambar H.8. Konfigurasi virtualbox.conf Langkah 4 ..... H-5
Gambar H.9. Konfigurasi processing.conf H-6
Gambar H.10. Konfigurasi memory.conf H-7
Gambar H.11. Konfigurasi reporting.conf H-8
Gambar I.1. *Disable the Windows Firewall* I-1
Gambar I.2. Instalasi *Guest Additional* Langkah 1 ..... I-2
Gambar I.3. Instalasi *Guest Additional* Langkah 2 ..... I-2
Gambar I.4. Instalasi *Guest Additional* Langkah 3 ..... I-3
Gambar I.5. *Setting up Host-only Networking* I-3
Gambar I.6. Konfigurasi IP Address Langkah 1 ..... I-4
Gambar I.7. Konfigurasi IP Address Langkah 2 ..... I-5
Gambar I.8. *Setting Up a Shared Folder* Langkah 1 ..... I-5
Gambar I.9. *Setting Up a Shared Folder* Langkah 2 ..... I-6
Gambar I.10. *Setting Up a Shared Folder* Langkah 3 ..... I-6
Gambar I.11. *Setting Up a Shared Folder* Langkah 4 ..... I-7
Gambar I.12. *Setting Up a Shared Folder* Langkah 5 ..... I-7
Gambar I.13. Instalasi agent Langkah 1 ..... I-8
Gambar I.14. Instalasi agent Langkah 2 ..... I-8
Gambar I.15. Instalasi agent Langkah 3 ..... I-9
Gambar I.16. Instalasi *Additional Software* I-9
Gambar J.1. *Setting up Host-only Networking* J-1
Gambar J.2. *Starting Cuckoo* J-1
Gambar J.3. *Starting Web Service Cuckoo* J-2
Gambar J.4. Tampilan *Web Service Cuckoo* J-2
Gambar J.5. *Command Starting Virtualbox* J-3
Gambar J.6. *Starting Virtualbox* J-3
Gambar J.7. *Select Malware* J-4
Gambar J.8. Proses Analisis Pada Terminal J-4
Gambar J.9. Proses Analisis Pada *Cuckoo Guest* J-5
Gambar J.10. Proses Analisis Pada *Web Service Cuckoo* J-5

DAFTAR LAMPIRAN

Lampiran A Instalasi Python Libraries A-1
Lampiran B Instalasi Virtualization Software B-1
Lampiran C Instalasi Django-based Web Interface C-1
Lampiran D Instalasi TCPdump D-1
Lampiran E Instalasi Volatility E-1
Lampiran F Instalasi Volatility Plug-ins F-1
Lampiran G Instalasi Mitmproxy G-1
Lampiran H Instalasi Configuration File H-1
Lampiran I Instalasi Configuration Guest OS I-1
Lampiran J Instalasi Simulasi J-1