

**PENGAMATAN MALWARE PADA VIRTUAL HONEYPOTS UNTUK
ANANLISIS PORT YANG DISERANG MALWARE**

Tugas Akhir



Oleh :

Giat Maradu Holong

22074365

Program Studi Teknik Informatika Fakultas Teknologi Informasi

Universitas Kristen Duta Wacana

Yogyakarta

2012

**PENGAMATAN MALWARE PADA VIRTUAL HONEYPOTS UNTUK
ANANLISIS PORT YANG DISERANG MALWARE**

Tugas Akhir



Diajukan kepada Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana

Sebagai salah satu syarat dalam memperoleh gelar

Sarjana Komputer

Disusun oleh :

Giat Maradu Holong

22074365

Program Studi Teknik Informatika Fakultas Teknologi Informasi

Universitas Kristen Duta Wacana

Yogyakarta

2012

PERNYATAAN KEASLIAN TUGAS AKHIR

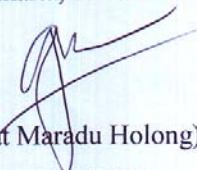
Saya menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul :

PENGAMATAN MALWARE PADA VIRTUAL HONEYPOTS UNTUK ANANLISIS PORT YANG DISERANG MALWARE

Yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan sarjana Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian sumber informasinya dicantumkan sebagaimana mestinya.

Jika kemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaaan saya.

Yogyakarta, 15 Januari 2013


(Giat Maradu Holong)

22074365

HALAMAN PERSETUJUAN

Judul : Pengamatan Malware pada Virtual Honeypots untuk Analisis
Port yang Diserang Malware
Nama : Giat Maradu Holong
NIM : 22074365
Mata Kuliah : Tugas Akhir
Kode : TIW276
Semester : Ganjil
Tahun Akademik : 2012/2013

UKDM
Telah diperiksa dan disetujui
Di Yogyakarta,
Pada tanggal 15 Januari 2013



Dosen Pembimbing I

Willy Sudiarto R, S.Kom., M.Cs.

Dosen Pembimbing II

Joko Purwadi, S.Kom., M.Kom.

HALAMAN PENGESAHAN

SKRIPSI

Pengamatan Malware pada Virtual Honeypots untuk Analisis Port yang Diserang
Malware

Dipertahankan di depan dewan penguji Tugas Akhir/Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu
Syarat memperoleh gelar
Sarjana Komputer Pada Tanggal


7 Januari 2013

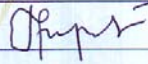
Yogyakarta, 16 Januari 2013


Mengesahkan,

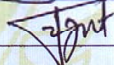
Dewan Penguji :

1. Willy Sudiarto R, S.Kom., M.Cs.
2. Joko Purwadi, S.Kom., M.Kom.
3. Nugroho Agus Haryono, S.Si., M.Si.
4. Antonius Rachmat C, S.Kom., M.Cs.











Dekan



(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Prodi

(Nugroho Agus Haryono, S.Si,M.Si)

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Ppenelitian dan laporan Tugas Akhir, yang berjudul Pengamatan Malware pada Virtual Honeypots untuk Analisis Port yang Diserang Malware.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah serta mampu memberikan informasi berkualitas sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan pembuatan program dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran dan masukan dari berbagai pihak, baik secara langsung maupun tidak langsung. Untuk itu pada kesempatan ini penulis ingin mengucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Budi Susanto S.Kom., M.T, OCA selaku Koordinator Tugas Akhir.
2. Bapak Willy Sudiarto R, S.Kom., M.Cs. selaku dosen pembimbing I yang dengan sabar membimbing, memberi semangat dan petunjuk kepada penulis selama penyusunan tugas akhir ini.
3. Bapak Joko Purwadi, S.Kom., M.Kom. selaku dosen pembimbing II atas bimbingan, petunjuk dan masukan yang diberikan selama pengerjaan tugas dari awal hingga akhir.
4. Keluarga tercinta, Ayah, Ibu, Kakak, dan Adik yang selalu memberikan semangat dan dukungan kepada penulis sehingga penulis dapat menyelesaikan tugas akhir.
5. Sahabat-sahabat penulis, Iswanto, Ricky Christie, Bosman Tambunan, Endra Dwi, Teman kost tercinta yang selalu memberikan semangat, hiburan dan berbagai masukan yang berguna bagi penulis.
6. Kepada internet, google maupun wikipedia yang telah membantu penulis dalam memahami materi.

7. Pihak - pihak lain yang tidak dapat penulis sebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa program dan laporan Tugas Akhir ini masih memiliki banyak kekurangan. Maka dari itu penulis sangat mengharapkan masukan berupa kritik dan saran yang bersifat membangun.

Akhir kata penulis ingin meminta maaf bila ada kesalahan baik dalam penyusunan laporan maupun yang pernah penulis lakukan sewaktu membuat program Tugas Akhir. Penulis juga berharap semoga laporan ini dapat bermanfaat bagi pembaca dan semua pihak yang berkepentingan dengan laporan ini.

Yogyakarta, 3 Desember 2012

Penulis



ABSTRAK

Penyebaran *malicious software* (malware) seiring waktu semakin banyak. *Update* terhadap celah keamanan yang diberikan vendor *software* tidak sepenuhnya menjadi jaminan pengguna terbebas dari masalah malware ini. Banyak kasus dimana pengguna yang memiliki sistem yang upto-date ataupun tidak mendapat serangan malware.

Jenis malware banyak yang tersebar di internet akan terus berkembang karena semakin banyak penggunanya. Perkembangan malware sendiri tidak dapat diprediksi secara pasti. Pembuat *software* tertentu akan berusaha untuk memperbaiki celah keamanan dan tidak tertutup kemungkinan tetap akan mendapatkan serangan dari jenis malware tertentu. Penulis akan mencoba mencatat statistik malware dengan menggunakan honeypot untuk mengetahui kebiasaan yang dimiliki malware tersebut.

Sistem yang dibangun berupa perangkat menggunakan honeypot yang dapat menangkap malware yang tersebar bebas di internet. Sistem ini mencatat semua serangan yang masuk kedalam honeypot. Penulis mengumpulkan malware sebanyak mungkin dan berhasil memperoleh data serangan malware terbesar berasal dari port HTTP.

Kata kunci : Honeypot, Malware.

DAFTAR ISI

HALAMAN SAMPUL DEPAN	
HALAMAN SAMPUL DALAM	
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
UCAPAN TERIMAKASIH.....	iv
ABSTRAK	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Metode Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA.....	7
2.1 Tinjauan Pustaka	7
2.2 Landasan Teori.....	9
2.2.1 Malware	9
2.2.1.1 Virus.....	10
2.2.1.2 Worm	12
2.2.1.3 Trojan Horse	12
2.2.1.4 Botnets	13
2.2.1.5 Spyware.....	14
2.2.2 Honeypot.....	15

2.2.2.1 Low-Interaction Honeypot	17
2.2.2.2 Honeyd	18
2.2.3 Analisis Malware	20
BAB III PERANCANGAN SISTEM	28
3.1 Kebutuhan Perangkat Keras dan Perangkat Lunak	28
3.1.1 Kebutuhan Perangkat Keras	28
3.1.2 Kebutuhan Perangkat Lunak	29
3.2 Perancangan Sistem dan Topologi	30
3.3 Tahapan Penelitian	33
3.3.1 Pengamatan Statistik pada Malware	33
3.3.2 Pengamatan pada Sandbox	33
3.3.3 Pengujian pada Sistem Real	34
BAB IV PENELITIAN	35
4.1 Implementasi	35
4.1.1 Linux Environment	35
4.1.2 Konfigurasi MikroTik	43
4.1.3 Windows Environment	48
4.2 Hasil Pengamatan	49
4.2.1 Pengamatan pada Honeypot	49
4.2.2 Pengamatan Malware Baru	52
4.2.3 Pengamatan pada Sistem Real	54
4.3 Analisis	54
4.3.1 Kendala yang Dihadapai	57
BAB V KESIMPULAN DAN SARAN	59
5.1 Kesimpulan	59
5.2 Saran	59

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR TABEL

Tabel 2.1 Keuntungan dan Kerugian <i>High-Interaction</i> dan <i>Low-Interaction</i> Honeypot	16
Tabel 2.2 Beberapa jenis <i>Low-Interaction</i> Honeypot	18
Tabel 4.1 Jenis Malware yang sudah <i>discan</i>	53

© UKDW

DAFTAR GAMBAR

Gambar 2.1 Struktur Botnet	14
Gambar 2.2 Ilustrasi Honeyd	19
Gambar 2.3 Modul pada Nepenthes.....	24
Gambar 2.4 Nepenthes Platform.....	25
Gambar 2.5 Skema Overview Sandbox	26
Gambar 3.1 Topologi I untuk Penelitian dengan IP NAT	31
Gambar 3.2 Topologi II untuk Penelitian Langsung dengan IP Publik	31
Gambar 4.1 Instalasi Nepenthes.....	35
Gambar 4.2 Log_Hexdump.....	36
Gambar 4.3 Download Manager pada Topologi I	37
Gambar 4.4 Download Manager pada Topologi II	37
Gambar 4.5 Nepenthes Ownership	38
Gambar 4.6 Firewall dan Service Firewall	39
Gambar 4.7 Interfaces Ubuntu pada Topologi I.....	40
Gambar 4.8 Interfaces Ubuntu pada Topologi II	40
Gambar 4.9 Restart Networking	41
Gambar 4.10 Routing Statis pada Topologi II	41
Gambar 4.11 Nepenthes setelah Dijalankan	42
Gambar 4.12 Netstat -antp	43
Gambar 4.13 Interfaces MikroTik.....	44
Gambar 4.14 IP Address I.....	45
Gambar 4.15 IP Address II.....	45

Gambar 4.16 Masquerade	46
Gambar 4.17 Routing OSPF	47
Gambar 4.18 DNS.....	47
Gambar 4.19 User	48
Gambar 4.20 XP dalam VMWare.....	49
Gambar 4.21 Log_Hexdump.....	50
Gambar 4.22 Contoh File Hexdump.....	50
Gambar 4.23 Log_Downloads	51
Gambar 4.24 Log_Submissions	52
Gambar 4.25 Binary	52
Gambar 4.26 Hasil Scan Binary.....	53
Gambar 4.27 Banyaknya Serangan Selama 3 Bulan.....	54
Gambar 4.28 Banyaknya Malware yang Berhasil Ditangkap.....	55
Gambar 4.29 Port yang Diserang.....	55
Gambar 4.30 Serangan pada Port yang Menghasilkan Malware	56
Gambar 4.3.1 Informasi Geografis Serangan.....	58

ABSTRAK

Penyebaran *malicious software* (malware) seiring waktu semakin banyak. *Update* terhadap celah keamanan yang diberikan vendor *software* tidak sepenuhnya menjadi jaminan pengguna terbebas dari masalah malware ini. Banyak kasus dimana pengguna yang memiliki sistem yang upto-date ataupun tidak mendapat serangan malware.

Jenis malware banyak yang tersebar di internet akan terus berkembang karena semakin banyak penggunaanya. Perkembangan malware sendiri tidak dapat diprediksi secara pasti. Pembuat *software* tertentu akan berusaha untuk memperbaiki celah keamanan dan tidak tertutup kemungkinan tetap akan mendapatkan serangan dari jenis malware tertentu. Penulis akan mencoba mencatat statistik malware dengan menggunakan honeypot untuk mengetahui kebiasaan yang dimiliki malware tersebut.

Sistem yang dibangun berupa perangkat menggunakan honeypot yang dapat menangkap malware yang tersebar bebas di internet. Sistem ini mencatat semua serangan yang masuk kedalam honeypot. Penulis mengumpulkan malware sebanyak mungkin dan berhasil memperoleh data serangan malware terbesar berasal dari port HTTP.

Kata kunci : Honeypot, Malware.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Permasalahan keamanan komputer yang paling banyak dijumpai adalah penyebaran *malicious software* (malware) di internet. Webserver adalah salah satu tempat penyebaran malware ini. Pengguna (*client*) yang mengakses webserver tersebut, mempunyai kemungkinan terjangkau oleh malware yang ada di webserver tersebut tanpa disadari. Kerugian yang disebabkan oleh serangan malware ini cukup banyak dan beragam. Penyebaran virus Brontok di Indonesia beberapa tahun lalu juga cukup marak dibicarakan. Kerugian yang disebabkan virus ini antara lain pengguna tidak dapat membuka *command prompt*, bahkan untuk beberapa varian akan langsung *re-start* komputer secara otomatis, *file/data* terhapus maupun rusak dan banyak lagi yang lainnya.

Vendor pembuat perangkat lunak tertentu, menyediakan *patch/update* untuk perangkat lunak yang mereka buat. *Patch* dibuat untuk memperbaiki celah keamanan pada perangkat lunak tertentu, salah satu contoh celah keamanan yang dimaksud adalah untuk mengatasi serangan bermacam-macam malware, misalnya Google Chrome yang merupakan salah satu contoh web browser, menyediakan update versi terbaru dan dalam versi ini browser ini memperbaiki celah keamanan pada fitur *password saving* dari serangan malware yang dapat mencuri *username* dan *password* pengguna. *Patch* yang disediakan oleh vendor pembuat perangkat lunak, tidak sepenuhnya dapat menjamin keamanan, karena perkembangan malware itu sendiri tidak dapat diprediksi secara pasti. Malware memiliki varian yang baru setiap saat. Pembuat malware selalu berusaha untuk mencari celah-celah keamanan (*vulnerabilities*) lainnya untuk *update malware* yang mereka buat. Komputer yang selalu *up-to-*

date (Sistem Operasi maupun perangkat lunak lain yang ada didalamnya) juga memiliki kemungkinan terjangkiti malware. Pengguna yang malas *meng-update* perangkat lunak yang mereka pakai, memiliki kemungkinan yang jauh lebih besar untuk terjangkit malware. Sebagian besar korban yang terinfeksi malware belum tentu mengetahui apa yang dilakukan malware terhadap komputer mereka masing-masing. Malware dapat menyusup lalu mencuri data pengguna, mencuri hak akses dan bahkan dapat merusak *file* yang ada didalam komputer pengguna. Menurut (Provos & Thosten, 2007), penyebaran dan perkembangan jenis malware baru sangat cepat, dan tidak dapat diketahui secara pasti, bahkan oleh vendor pembuat antivirus sekalipun. Berdasarkan data statistik, waktu yang dibutuhkan malware menginfeksi komputer yang tidak di *patch* (Windows XP) hanya 5 sampai 10 menit saja.

Penulis akan melakukan penelitian yang berupa mengumpulkan beberapa tipe malware dari internet menggunakan Honeypot. Malware yang dikumpulkan tersebut akan dicatat (dilakukan pengamatan). Penulis juga akan melakukan pengamatan terhadap tingkahlaku (*behavior*) malware terhadap sistem yang diserang, dan bagian apa saja yang paling sering diserang terhadap sebuah sistem, sehingga dapat diketahui jenis malware yang paling berbahaya sampai yang tidak berbahaya.

1.2 Perumusan Masalah

Berdasarkan latarbelakang permasalahan di atas, adapun perumusan masalah yang akan diteliti antara lain :

- a. Bagaimana membuat sebuah sistem yang tepat, yang didalamnya terintegrasi dengan honeypot, dan akan dipakai untuk mengumpulkan malware.
- b. Bagaimana cara mengetahui port yang paling sering digunakan dalam penyebaran malware.
- c. Bagaimana mengetahui sumber serangan malware (berdasarkan geografis).

1.3 Batasan Masalah

Adapun batasan permasalahan yang akan digunakan untuk penelitian ini adalah sebagai berikut:

- a. Penulis melakukan penelitian ini hanya untuk melakukan pengamatan, dan pengamatan terhadap port yang diserang bukan untuk memperbaiki sistemnya.
- b. Penulis melakukan penelitian hanya pada lingkup server DWTC.
- c. Penulis hanya meneliti malware yang didapatkan dari honeypot, dan jika ada malware yang lain diluar itu, hanya dipakai untuk acuan pembelajaran.
- d. Honeypot yang dibangun merupakan *low-interaction* honeypot.
- e. Malware dinyatakan sebagai malware baru jika tidak berhasil diidentifikasi oleh antivirus

1.4 Tujuan Penelitian

Berdasarkan permasalahan diatas, adapun tujuan dari penelitian yang akan dilakukana adalah sebagai berikut :

- a. Untuk melakukan pengamatan terhadap malware yang ditangkap honeypot. Malware tersebut akan diteliti lebih lanjut dari beberapa aspek misalnya kebiasaannya dalam menyerang port.
- b. Penulis ingin mengumpulkan informasi mengenai malware guna mengetahui tentang malware lebih spesifik.
- c. Penulis ingin mnegetahui negara mana saja yang paling banyak melakukan penyerangan terhadap sistem.

1.5 Metode Penelitian

Adapun metode penelitian yang akan digunakan dalam pengumpulan malware dan analisis malware adalah sebagai berikut:

a. Studi Pustaka

Studi pustaka bertujuan untuk mengumpulkan semua bahan teori yang berhubungan dengan malware, honeypot, dan Sandbox. Bahan teori dapat bersumber dari jurnal, buku, maupun media internet. Bahan teori ini ditujukan sebagai bahan dasar dan acuan pembandingan pada saat implementasi di lapangan.

b. Praktek lapangan

Praktek dilapangan adalah membangun sistem untuk penelitian, meliputi beberapa hal antara lain sebagai berikut :

- Membuat topologi : menentukan topologi yang cocok untuk sistem honeypot yang akan dibangun.
- Membangun Sistem : pada tahap ini, akan dibangun sebuah server untuk honeypot. *Server* adalah objek yang akan diserang oleh malware. Server ini dapat berupa mail sever, web server dan lainnya. Server virtual honeypot akan diintegrasikan dengan layanan (service) mail atau layanan lainnya. Sistem ini akan berfungsi sebagai pendeteksi adanya serangan malware dan sekaligus sebagai alat untuk menangkap malware.
- Baselining Sistem : pada tahap ini dilakukan semua pencatatan tentang keadaan pada komputer server dan jaringannya. Baseline ini dapat berupa mencatat semua service yang berjalan pada server. Misalnya : pengguna dan grup yang aktif ataupun tidak, port yang dijalankan pada server, *filesistem* yang dipakai pada server, sistem registry. Dalam lalulintas (*traffic*) jaringan menggunakan wireshark untuk mengamati jaringan dan semua *traffic* keluar masuk ke server.

- Mengumpulkan Informasi : pada tahap ini semua sistem sudah siap, akan dijalankan dan dihubungkan dengan internet (publik). Semua aktivitas yang terjadi didalam jaringan akan dicatat dan dimasukkan kedalam *log*. Pada tahap ini juga akan dicatat ada berapa banyak malware yang keluar masuk server, berapa banyak yang melakukan penyerangan terhadap server, apa saja yang diserang dan perubahan apa saja yang terjadi pada server tersebut. Pada tahap ini juga akan dilakukan penelitian lebih lanjut terhadap malware. Penelitian lebih lanjut terhadap malware menggunakan Sandbox.
- Menganalisis informasi : setelah semua informasi diatas dicatat, penulis akan menganalisis informasi tersebut. Penulis akan mengelompokkan jenis – jenis malware pada kategori tertentu, misalnya : worm, trojan horse, virus dan lainnya. Setelah dikelompokkan akan dikelompokkan lagi kedalam jenis bahayanya.
- Dokumentasi hasil : pada tahap ini, semua hasil dari penelitian diatas akan dibuat dalam bentuk laporan.

1.6 Sistematika Penulisan

Penulisan laporan tugas akhir ini terdiri dari 5 bagian utama. Bab 1 merupakan pendahuluan, yang berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penulisan dan sistematika penulisan. Bab 1 juga memberikan gambaran umum mengenai penelitian tugas akhir ini.

Bab 2 merupakan tinjauan pustaka, yang berisi tentang landasan teori yang mendasari perancangan dan pembuatan sistem. Pada bab ini landasan teori akan membahas mengenai honeypot dan prinsip dasarnya, malware dan beberapa jenis-jenis malware.

Bab 3 akan membahas tentang perancangan sistem secara keseluruhan, yang meliputi topologi yang akan dipakai dalam penelitian, dan teknik yang akan dipakai dalam mengumpulkan dan meneliti malware.

Bab 4 berisi tentang hasil implementasi dan analisis sistem. Bab ini meliputi sistem *real* yang telah dibuat lengkap beserta penjelasan dan analisisnya.

Bab 5 adalah bagian terakhir dari laporan. Bab ini berisi kesimpulan dan saran. Kesimpulan merupakan jawaban dari pertanyaan penelitian yang ditanyakan dalam perumusan masalah, sedangkan saran berisi kesimpulan yang perlu ditindaklanjuti atau direalisasikan dikemudian hari.

© UKDW

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pengamatan yang sudah dilakukan, kesimpulan yang dapat ditarik dari penelitian ini adalah :

- a. Autonomous malware tidak menyerang semua publik, sehingga ada beberapa IP hanya mendapatkan sedikit serangan bahkan tidak mendapatkan serangan sama sekali. Untuk mendapatkan serangan yang banyak dibutuhkan jaringan yang memiliki *traffic* jaringan yang tinggi, karena semakin tinggi *trafficnya* akan semakin tinggi juga ketertarikan seseorang untuk melakukan tindakan penyerangan.
- b. Banyaknya *vulnerabilities* yang terdapat pada sebuah sistem mempengaruhi jumlah serangan yang ada.
- c. Sedikitnya jumlah serangan yang didapatkan menyebabkan sedikitnya malware yang dikumpulkan dan semakin kecil pula kemungkinan untuk memperoleh malware baru (zero day malware) sangat kecil.
- d. Serangan terbesar pada sistem ini berasal dari HTTP yaitu 63% dari total serangan dan serangan terbesar kedua berasal dari creceive yaitu 25% dari total serangan.
- e. Sebagian besar malware yang dikumpulkan berasal dari serangan yang menggunakan port creceive yaitu 70% dari total malware.
- f. Sebagian besar serangan berasal dari Amerika yaitu 50% dari total serangan, kemudian Rusia sebesar 14% dan Jepang 13% dari total serangan.
- g. Sebagian besar malware yang tersebar di internet masih didominasi oleh malware lama.

- h. Penggunaan sistem langsung seperti pada topologi kedua lebih efektif dibandingkan dengan sistem virtual seperti pada topologi pertama. Pada topologi pertama tidak ditemukan adanya serangan sedangkan pada topologi kedua ditemukan beberapa serangan dan berhasil mengumpulkan malware.

5.2 Saran

Adapun saran-saran yang dapat digunakan untuk penelitian lebih lanjut antara lain :

- a. Nepenthes sudah tidak *disupport* lagi sehingga update *vulnerability* yang baru ditemukan tidak akan tersedia untuk sistem ini. Untuk penelitian lebih lanjut penulis menyarankan menggunakan Dionaea yang merupakan penyempurnaan dari nepenthes.
- b. Untuk penelitian malware lebih lanjut selain *behavior* analysis dapat dilakukan *code* analysis namun penelitian ini akan lebih sulit dan kompleks.
- c. Penggunaan IP publik yang memiliki traffic tinggi sangat disarankan untuk sistem ini, karena sering diakses dan banyak yang mengetahuinya sehingga kemungkinan penyebaran malware lebih tinggi.
- d. Untuk memaksimalkan sistem honeypot, dibutuhkan sistem terdistribusi.

DAFTAR PUSTAKA

Baecher, P., Koetter, M., Holz, T., Dorsneif, M., & Freiling, F. (2006). The Nepenthes Platform: An Efficient Approach to Collect Malware. *LNCS*, 165-184.

Provos, N., & T. H. (2007). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Boston: Addison Wesley.

Szor, P. (2005). *The Art of Computer Virus Research and Defense*. Boston: Addison Wesley Professional.

Zelster, L. (2009). Introduction to Malware Analysis.

Zhuge, J., Holz, T., Han, X., Song, C., & Zou, W. (2007). Collecting Autonomous Spreading Malware using High-Interaction Honeypots.

© UKDWN