TUGAS AKHIR

EKSPLORASI MALWARE POISON IVY MENGGUNAKAN METODE MALWARE ANALISIS DINAMIS DAN MALWARE ANALISIS STATIS

DARMAWAN RAMADANA

12 1065 1040

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2016

HALAMAN PENGESAHAN

EKSPLORASI MALWARE POISON IVY MENGGUNAKAN METODE MALWARE ANALISIS DINAMIS DAN MALWARE ANALISIS STATIS

Oleh :

DARMAWAN RAMADANA

12 1065 1040

Telah Mempertanggung Jawabkan Laporan Tugas Akhir Pada Siding Tugas Akhir Tanggal 26 Juli 2016 Sebagai Salah Satu Syarat Kelulusan Dan Mendapatkan Gelar Sarjana Komputer (S.Kom)

di

Universitas Muhammadiyah Jember

Disetujui oleh :

Dosen Penguji :	Dosen Pembimbing :
Penguji I	Pembimbing I
Yeni Dwi Rahayu, S. ST., M. Kom.	**Triawan Adi Cahyanto., M.Kom**
NIDN. 0716108602	NPK. 1203719
Penguji II	Pembimbing II
Daryanto., M.Kom	**Victor Wahanggara., M. Kom.**
NPK. 1103589	NPK. 1209739
Mengesahkan,	Mengetahui,
Dekan Fakutas Teknik	Ketua Program Studi Teknik Informatika
Ir. Suhartinah, MT.	**Yeni Dwi Rahayu, S. ST., M. Kom.**
NPK. 9505246	NIDN. 0716108602

KATA PENGANTAR

Bismillahirrahmanirrahim

Puji syukur kehadirat Allah SWT yang Maha Pengasih lagi Maha Penyayang, Yang hanya kepadaNya-lah segala sesuatu bergantung. Alhamdulillah tak lupa senantiasa saya panjatkan karena hanya dengan ridho, kemurahan dan kekuasaanNya-lah proyek akhir yang berjudul:

"EKSPLORASI MALWARE POISON IVY MENGGUNAKAN METODE MALWARE ANALISIS DINAMIS DAN MALWARE ANALISIS STATIS"

dapat diselesaikan dengan segala kelebihan dan tak lepas dari kekurangan yang terdapat di dalamnya.

Shalawat serta salam semoga senantiasa tercurah kepada baginda Rasulullah Muhammad SAW, keluraga beliau dan para sahabat hingga pengikutnya hingga akhir zaman, orang-orang yang senantiasa istiqomah menegakkan kebenaran dan menebar kebaikan di bumi Allah SWT.

Proyek akhir ini menjelaskan tentang bagaimana mengeksplorasi program malware poison ivy menggunakan metode malware analisis dinamis dan malware analisis statis.

Dengan segala kerendahan hati, penulis memohon maaf jika ternyata di kemudian hari diketahui bahwa hasil dari proyek akhir ini masih jauh dari kesempurnaan. Semoga bermanfaat bagi setiap insan yang mempergunakannya untuk kebaikan di jalan Allah SWT.

Jember, 1 Agustus 2016

Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN MOTTO ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN iv
ABSTRAK v
ABSTRACT vi
HALAMAN PERSEMBAHAN vii
KATA PENGANTAR viii
HALAMAN UNGKAPAN TERIMA KASIH ix
DAFTAR ISI x
DAFTAR GAMBAR xiii
DAFTAR TABEL xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 3
1.5 Maftaar Penelitian 3
BAB II TINJAUAN PUSTAKA 4
2.1 Penelitian Terdahulu 4
2.2 Landasan Teori 5
2.2.1 Malware 5
1. Malware yang menginjeksi perangkat lunak 5
a.Virus 5
b.Worm 6
2. Malware yang mencari dan mencuri keuntungan 6
a. Spyware 6
b. Adware 6
c. Keystroke Logger 7

d. Dialer 7
3. Malware yang bersembunyi didalam perangkat komputer 8
a. Trojan Horse 8
b. Rootkit 8
c. Backdoor 8
2.2.2 Poison Ivy RAT (Remote Access Trojan) 9
2.2.3 Metode Malware Analisi
a. Malware Analisis Dinamis 9
b. Malware Analisis Satis 10
c. Virtual Machine 10
d. Oracle VM Virtualbox 10
e. Cuckoo Sandbox 11
f. Reghost 12
g. Wireshark 12
h. Volatolity Framework 13
i. IDA Pro 13
BAB III METODOLOGI 14
3.1 Metode Penelitian 14
3.2 Studi Literatur 14
3.3 Analisis 15
3.3.1 Analisis Kebutuhan 16
3.3.2 Tahapan Malware Analisis Dinamis 16
3.3.2.1 Membangun Virtual Lab 16
3.3.2.2 Menjalankan Malware 23
3.3.2.3 Analisis Perilaku Malware 24
3.3.2.4 Analisis Malware Otomatis (Cuckoo Sandbox) 25
3.3.3 Tahapan Malware Analisis Statis 30
3.3.3.1 Ekstraksi File Malware 30
3.3.3.2 Analisis Perilaku (Kode) 31
3.3.3.3 Disassember 31
3.3.4 Hasil Pengujian dan Analisis 31

3.4 Laporan 32
3.5 Waktu Pelaksanaan Penelitian 20

BAB IV PEMBAHASAN 33
4.1 Pengujian dan Analisis 33
4.1.1 Pengujian dan Analisis Malware Dinamis 33
a. Pengujian Virtual Lab 33
b. Analisis Perilaku Menggunakan Regshot 34
c. Analisis Perilaku Menggunakan Cuckoo Sandbox 37
d. Analisis Paket Jaringan Program Malware Poison Ivy Menggunakan Wireshark 41
4.1.2 Analisis Malware Statis 46
a. Ekstraksi (Decompile) Program Ivy Kode String Menggunakan Program Strings Kali Linux 46
b. Ekstraksi (Disassembly) Program Poison Ivy Menggunakan IDA Pro 49
4.2 Hasil Temuan pada Pengujian dan Analisis 53
BAB V KESIMPULAN DAN SARAN 55
5.1 Kesimpulan 55
5.2 Saran 56
DAFTAR PUSTAKA 57

DAFTAR GAMBAR

Gambar 3.1 Alur Metode Penelitian 14
Gambar 3.2 Skema Analisis *Malware* 15
Gambar 3.3 Proses Instalasi *VirtualBox* 17
Gambar 3.4 Proses Instalasi *VirtualBox* Selesai 18
Gambar 3.5 Jendela Utama *VirtualBox* 18
Gambar 3.6 Tombol Membuat Virtual Mesin Baru 19
Gambar 3.7 Jendela Pengaturan nama baru pada virtual mesin 19
Gambar 3.8 Jendela Pengalokasian Ukuran *Virtual RAM* 19
Gambar 3.9 Jendela *Virtual Hardisk* 20
Gambar 3.10 Jendela Tipe *Virtual Hardisk* 20
Gambar 3.11 Jendela Pengalokasian Ukuran *Virtual Hardisk* 21
Gambar 3.12 *Menu* Pengaturan *Virtualbox* 21
Gambar 3.13 Sub *Menu* 22
Gambar 3.14 *Menu Start* 22
Gambar 3.16 Topologi Arsitektur Jaribang *Virtual Lab* 22
Gambar 3.17 Pengaturan Alamat IP *Vboxnet* (*Kali Linux*) 23
Gambar 3.18 Pengaturan Alamat IP Komputer *Server* 23
Gambar 3.19 Pengaturan Alamat IP Komputer Klien 23
Gambar 3.20 Daftar Kartu Jaringan *Wireshark* 24
Gambar 3.21 *File* pengaturan *Cuckoo Sandbox* 25
Gambar 3.22 Pencarian Lokasi *tcpdump* 26
Gambar 3.23 Pengaturan *File* auxiliary.conf 27
Gambar 3.24 Pengaturan *File* cuckoo.conf 27
Gambar 3.25 Pengaturan *File* kvm.conf 28
Gambar 3.26 Pengaturan *File* processing.conf 29
Gambar 3.27 Pencarian Lokasi *Vboxnamage* 29
Gambar 3.28 Pengaturan *File* virtualbox.conf 30
Gambar 4.1 Menjalankan Windows SP pada Kali Linux 33
Gambar 4.2 Proses menjalankan program *malware poison ivy* 34

Gambar 4.3 Aplikasi Regshot 34
Gambar 4.4 Menu Regshot pada 1st shot 35
Gambar 4.5 Pengambilan shot kedua 35
Gambar 4.6 Menu Compare pada Regshot 36
Gambar 4.7 Menjalankan Program *Cuckoo sandbox* 37
Gambar 4.8 Melakukan eksekusi program *malware* pada mesin *cuckoo sandbox* 37
Gambar 4.9 Analisis *Malware Cuckoo Sandbox Agent* 38
Gambar 4.10 Program poison ivy terkoneksi dengan program induk 41
Gambar 4.11 Remote Shell Komputer Server Oleh Komputer Klien 42
Gambar 4.12 Hasil Capture Wireshark pada Percobaan1 42
Gambar 4.13 Data Lengkap Protokol *TCP* dari Data Paket Nomor 1 (Gambar 4.46). 43
Gambar 4.14 Hasil Capture Wireshark pada Percobaan2.dari Data paket nomor 1..... 44
Gambar 4.16 Data Lengkap *Protocol ICMP Request* dari paket data nomor 8 (Gambar 4.47) 45
Gambar 4.17 Data Lengkap Protocol ICMP Replay dari paket data nomor 9 (Gambar 4.46) 45
Gambar 4.18 Kode String Program Malware Poison Ivy 47
Gambar 4.19 Percobaan Autentikasi Sampel Malware Poison Ivy 49
Gambar 4.20 Temuan Kode String “pi_agent” pada IDA Pro 51
Gambar 4.21 Temuan Kode String “192.168.56.20” pada IDA Pro 51
Gambar 4.22 Temuan Kode String “secret_agent” pada IDA Pro 52

DAFTAR TABEL

Tabel 4.1 Temuan proses *compare regshot* 36
Tabel 4.2 Informasi *file* program *malware poison ivy* 39
Tabel 4.3 Temuan perilaku program *malware poison ivy* pada *cuckoo sandbox* 39
Tabel 4.4 Temuan kode string hasil ekstraksi menggunakan program strings 47
Tabel 4.5 Konversi Bilangan (Character Code 32 – 127) 49
Tabel 4.2 Hasil Temuan dari Pengujian dan Analisis Program Malware Poison Ivy . 53

DAFTAR LAMPIRAN

LAMPIRAN

Lampiran 1

DAFTAR PUSTAKA

Ari Nugroho, Prayudi, 2015, *Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan Malware*, Makalah KNSI 2014.

Distler, D. 2007. *Malware Analysis: An Introduction*. Jurnal of SANS Institute. December, 2007.

Indriantono, N. Supomo B., (1999), *Methodologi Penelitian Bisnis untuk Akuntansi & Manajemen*, Yogyakarta, BPFE.

(*IANA*, 2016) http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml (diakses 13 Mei 2016).

Kramer, S., and Bradfield, J. C. (2009). *A general definition of malware. Journal in Computer Virology*. 6(2), 105-114. Doi:10.1007/s11416-009-0137-1

Kurniawan, 2012, *Network Forensics:* Panduan analisis & Investigasi Paket Data Jaringan menggunakan *Wireshark*, ANDI.

R. Perdhana, 2011, *Harmless Hacking: Malware Analysis dan Vulnerability Development*, GrahaIlmu.

Wahanggara dan Prayudi, 2015, *Sistem Deteksi Malicious Software Berbasis System Call untuk Klasifikasi Barang Bukti Digital Menggunakan Metode Support Vector Machine*, Seminar Teknologi dan Rekayasa ISSN.

Yusirman S, Prayudi dan Riadi, 2015, *Implementation of Malware Analysis using Static and Dynamic Analysis Method*, International Journal of Computer Applications Vol. 117. No.6.

(Yovisto, 2015) http://blog.yovisto.com/fred-cohen-and-the-first-computer-virus/ (diakses 10 Januari 2016).

(_____, 2005) http://www.ascii-code.com/ (diakses 20 Mei 2016).