SISTEM IDENTIFIKASI *MALWARE* MENGGUNAKAN METODE *SIGNATURE-BASED YARA* UNTUK *WEBSITE* BERBASIS *PHP*

DHENY PRIATNA
41511120041

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2017

SISTEM IDENTIFIKASI *MALWARE* MENGGUNAKAN METODE *SIGNATURE-BASED YARA* UNTUK *WEBSITE* BERBASIS *PHP*

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Persyaratan
Menyelesaikan Gelar Sarjana Komputer

DHENY PRIATNA

41511120041

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA

2017

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM	:	41511120041
Nama	:	Dheny Priatna
Judul Tugas Akhir	:	Sistem Identifikasi Malware Menggunakan Metode Signature-based YARA untuk Website Berbasis PHP

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 19 Juli 2017

Dheny Priatna

LEMBAR PENGESAHAN

Nama	:	Dheny Priatna
NIM	:	41511120041
Jurusan	:	Teknik Informatika
Fakultas	:	Ilmu Komputer
Judul	:	Sistem Identifikasi Malware Menggunakan Metode Signature-based YARA untuk Website Berbasis PHP

Jakarta, 19 Juli 2017

Disetujui dan diterima oleh,

Drs. Achmad Kodar, MT., Mkom.

Dosen Pembimbing

Desi Ramayanti,. S.Kom., MT.

Kaprodi Teknik Informatika

Diky Firdaus, S.Kom., MM.

Koordinator Tugas Akhir

KATA PENGANTAR

Puji Syukur dipanjatkan kehadirat Allah SWT, karena atas karunia yang telah diberikan kepada-Nya sehingga dapat diselesaikan Laporan Tugas Akhir tepat pada waktunya, Laporan Tugas Akhir tersebut merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Tugas Akhir ini takkan dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati diucapkan terima kasih kepada:

1. Bapak Drs, Achmad Kodar, MT., Mkom selaku Pembimbing Tugas Akhir yang telah membimbing dengan semua nasihat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Ibu Desi Ramayanti,. S.Kom., MT. selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana
3. Bapak Diky Firdaus, S.Kom., MM selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana.
4. Keluarga besar terutama Bapak, Ibu, dan Adik yang telah memberikan doa dan dukungannya.
5. Istri tercinta Ria Indriani yang selalu memberikan dukungan serta semangatnya
6. Beserta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin.

Jakarta, 2 Juni 2016

Dheny Priatna

DAFTAR ISI

JUDUL i
LEMBAR PERNYATAAN ii
LEMBAR PENGESAHAN iii
KATA PENGANTAR iv
ABSTRACT v
ABSTRAK vi
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xii

BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Identifikasi Masalah 3
1.3 Rumusan Masalah 3
1.4 Batasan Masalah 3
1.5 Tujuan Penelitian 3
1.6 Manfaat Penelitian 4
1.7 Sistematika Penulisan 4
1.8 Metode Penelitian 5

BAB II LANDASAN TEORI 6
2.1 Perangkat Perusak (*Malware*) 6
2.1.1 Survey *Malware* (*Malware Trends*) 6
2.1.2 Klasifikasi *Malware* 7
2.1.3 Sasaran *Malware* 8
2.2 Pusat Data (*Data Center*) 10
2.2.1 Peladen (*Server*) 11
2.2.2 Situs Web (*Website*) 11
2.3 Detektor *Malware* (*The Malware Detector*) 12
2.3.1 Teknik Deteksi *Malware* 12
2.4 YARA 16
2.4.1 Cara Kerja YARA 17
2.4.2 Modul YARA 19

2.4.3 Menggunakan YARA dari Python 20
2.5 Metrik Keamanan (*Security Metrics*) 20
2.6 *Unified Modeling Language* (UML) 21

BAB III ANALISA DAN PERANCANGAN 23
3.1 Analisa Pembuatan Sistem 23
3.1.1 Analisa Pengguna 23
3.1.2 Analisa Kebutuhan 24
3.1.3 Spesifikasi Kebutuhan Sistem 24
3.2 Kerangka Pemikiran 25
3.3 Perancangan Sistem yang Diajukan 26
3.3.1 Desain Komponen dan Inti Sistem yang Diajukan 26
3.3.2 Desain Topologi 27
3.3.3 Diagram Proses Implementasi Sistem 28
3.3.4 Diagram *Use Case* 29
3.3.5 Diagram Aktifitas 32
3.3.5.1 Diagram Aktifitas "Tambah *Rules* 32
3.3.5.2 Diagram Aktifitas "Tambah *Librari*" 33
3.3.5.3 Diagram Aktifitas "Tambah Klien" 33
3.3.5.4 Diagram Aktifitas "Hapus *Rules*" 34
3.3.5.5 Diagram Aktifitas "Hapus Librari" 35
3.3.5.6 Diagram Aktifitas "Hapus Klien" 35
3.3.5.7 Diagram Aktifitas "*Scan Malware*" 36
3.3.5.8 Diagram Aktifitas "Karantina" 37
3.3.5.9 Diagram Aktifitas "Update Sistem" 37
3.3.5.10 Diagram Aktifitas "Setel *Whitelist*" 38
3.3.5.11 Diagram Aktifitas "Setel Direktori" 39

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM 40
4.1 Konfigurasi Sistem Operasi pada Server 40
4.1.1 Persiapan Sistem (Prerequisites) 40
4.2 Konfigurasi Sistem Identifikasi *Malware* YARA 41
4.2.1 Kompilasi Sistem 41
4.2.2 Konfigurasi Pemasangan Sistem 41
4.2.3 Konfigurasi Direktori Sistem 42
4.3 Tampilan dan Cara Kerja Sistem 43
4.3.1 Tampilan Informasi Sistem 43
4.3.2 Tampilan *Rules* 44
4.3.3 Tampilan Librari *Rules* 45
4.3.4 Tampilan *Client* 45
4.3.5 Tampilan *Scan* 46
4.3.6 Tampilan Karantina 50
4.3.7 Tampilan *Whitelist* 57
4.3.8 Tampilan Setel Direktori 58
4.4 Pengujian Sistem 59
4.4.1 Hasil Pengujian Fungsionalitas 60
4.4.2 Hasil Pengujian Kualitas 62

BAB V PENUTUP 67
5.1 Kesimpulan 67
5.2 Saran 67
DAFTAR PUSTAKA 68
LAMPIRAN A *Sourcecode Program* 69
LAMPIRAN B *Sourcecode Malware* 88

DAFTAR GAMBAR

Gambar 1. Alur Penelitian 5
Gambar 2. Malware Trends 6
Gambar 3. Klasifikasi Malware 7
Gambar 4. Teknik Deteksi Malware 13
Gambar 5. Algoritma YARA dalam Flowcart 18
Gambar 6. Kerangka Pemikiran 25
Gambar 7. Desain Komponen dan Inti Sistem yang Diajukan 26
Gambar 8. Desain Topologi Sistem yang Diusulkan 27
Gambar 9. Diagram Implementasi Sistem 28
Gambar 10. Diagram Use Case Sistem Identifikasi Malware 29
Gambar 11. Diagram Aktifitas “Tambah Rules 32
Gambar 12. Diagram Aktifitas “Tambah Librari” 33
Gambar 13. Diagram Aktifitas “Tambah Klien” 34
Gambar 14. Diagram Aktifitas “Hapus Rules” 34
Gambar 15. Diagram Aktivitas “Hapus Librari” 35
Gambar 16. Diagram Aktifitas “Hapus Klien” 36
Gambar 17. Diagram Aktifitas “Scan Malware” 36
Gambar 18. Diagram Aktifitas “Karantina” 37
Gambar 19. Diagram Aktifitas “Update” 38
Gambar 20. Diagram Aktifitas “Setel Whitelist” 39
Gambar 21. Diagram Aktivitas “Setel Direktori” 39
Gambar 22. Sistem Operasi yang Diinstal 40
Gambar 23. Konfigurasi File Sistem Identifikasi 42
Gambar 24. Konfigurasi Folder Sistem Identifikasi 42
Gambar 25.Pengetesan Instalasi Sistem Identifikasi 43
Gambar 26.Tampilan Awal Sistem Identifikasi Malware 43
Gambar 27.Tampilan Rules 44
Gambar 28.Tampilan Librari Rules 45
Gambar 29.Tampilan Penambahan Librari Rules 45
Gambar 30.Tampilan Tambah Client 46
Gambar 31.Tampilan Scan Sistem 46
Gambar 32.Tampilan Scan Sistem saat Berjalan Mendeteksi 50
Gambar 33.Tampilan Whitelist 57

Gambar 34.Tampilan Input Whitelist 58
Gambar 35.Tampilan Setel Direktori 58
Gambar 36.Notifikasi Error Setel Direktori 58
Gambar 37. Hasil Uji Pertama 64
Gambar 38. Hasil Uji Kedua 66

DAFTAR TABEL

Tabel 1. Tabel Pengguna 22
Tabel 2. Spesifikasi Kebutuhan Sistem 24
Tabel 3. Spesifikasi Kebutuhan Tambahan 25
Tabel 4. Use Case “Tambah Rules” 29
Tabel 5. Use Case “Tambah Librari” 29
Tabel 6. Use Case “Tambah Klien” 29
Tabel 7. Use Case “Hapus Rules” 29
Tabel 8. Use Case “Hapus Librari” 29
Tabel 9. Use Case “Hapus Klien” 30
Tabel 10. Use Case “Scan Malware” 30
Tabel 11. Use Case “Karantina” 30
Tabel 12. Use Case “Update Sistem” 30
Tabel 13. Use Case “Setel Whitelist” 30
Tabel 14. Use Case “Setel Direktori” 31
Tabel 15. Data Penguji 59
Tabel 16. Pengujian Fungsionalitas Sistem Identifikasi Malware 60
Tabel 17. Sistematika Pengujian 63
Tabel 18. Sampel Malware 63
Tabel 19. Sampel File Yang Disisipkan Malware 64
Tabel 20. Analisa Hasil Pengujian 6