

DAFTAR ISI

HALAMAN JUDUL.....	ii
LEMBAR PENGESAHAN.....	iii
LEMBAR PERNYATAAN.....	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	x
DAFTAR LAMPIRAN.....	xi
INTISARI.....	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Sistematika Penulisan.....	2
BAB II TINJAUAN PUSTAKA	4
2.1 Lingkup Tinjauan Pustaka	4
2.2 Landasan Teori.....	7
2.2.1 <i>Honeypot</i>	7
2.2.2 <i>Dionaea Honeypot</i>	7
2.2.3 <i>Hashing untuk Malware Fingerprint</i>	8
2.2.4 <i>Yara</i>	8
2.2.5 <i>Signature-based Malware Detection</i>	8
2.2.6 <i>MongoDB sebagai Database Log Serangan Honeypot</i>	9
2.2.7 <i>Mosquitto MQTT Broker</i>	10
2.2.8 <i>Metrik Evaluasi Akurasi Pendeteksian Malware</i>	10
2.3 Hipotesis	12
BAB III BAHAN DAN METODOLOGI PENELITIAN	14
3.1 Bahan	14
3.2 Peralatan.....	15
3.3 Tahapan Penelitian	16
3.4 Perancangan Alat	18



3.4.1	Perancangan Sistem.....	18
3.4.2	Instalasi dan Konfigurasi Sistem.....	22
3.5	Pengujian Sistem.....	35
3.5.1	Pengujian Fungsionalitas Sistem.....	35
3.5.2	Pengujian Akurasi Pendeteksian <i>Malware</i>	37
3.5.3	Pengujian <i>Multi Client</i> Pendeteksian <i>Malware</i>	37
3.5.4	Pengujian Antisipasi Kesalahan Deteksi saat <i>Client Offline</i>	38
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		39
4.1	Pengujian Fungsionalitas Sistem	39
4.1.1	Fungsi <i>Collecting Data Honeypot</i>	39
4.1.2	Fungsi <i>Collecting Data Hash Client File</i>	42
4.1.3	Fungsi <i>Top-Down Malware Detection</i>	45
4.2	Pengujian Akurasi Pendeteksian <i>Malware</i>	47
4.2.1	<i>True Positive Rate (TPR)</i>	47
4.2.2	<i>True Negative Rate (TNR)</i>	47
4.2.3	<i>False Positive Rate (FPR)</i>	47
4.2.4	<i>False Negative Rate (FNR)</i>	48
4.3	Pengujian <i>Multi Client Malware Detection</i>	48
4.4	Pengujian Antisipasi Kesalahan Deteksi saat <i>Client Offline</i>	50
BAB V PENUTUP		52
5.1	Kesimpulan	52
5.2	Saran	52
DAFTAR PUSTAKA		54
LAMPIRAN		56

DAFTAR GAMBAR

Gambar 2.1 <i>Structure Embedded Document</i>	9
Gambar 2.2 <i>Strucure Referenced Document</i>	10
Gambar 3.1 <i>Flowchart</i> tahapan penelitian	16
Gambar 3.2 Diagram sistem <i>bottom-up malware detection</i>	19
Gambar 3.3 Topologi Jaringan Sistem <i>Malware Detection Top-Down</i>	19
Gambar 3.4 Diagram sistem <i>top-down malware detection</i>	20
Gambar 3.5 <i>Flowchart</i> cara kerja sistem <i>top-down malware detection</i>	21
Gambar 3.6 Perintah pengunduhan paket <i>dionaea honeypot</i>	23
Gambar 3.7 <i>Deployment dionaea honeypot</i>	24
Gambar 3.8 <i>File</i> konfigurasi modul harvester	24
Gambar 3.9 <i>File service</i> modul harvester	25
Gambar 3.10 Perintah menjalankan modul harvester	25
Gambar 3.11 Instalasi mosquito MQTT <i>broker</i>	26
Gambar 3.12 Instalasi docker	28
Gambar 3.13 Instalasi MongoDB	29
Gambar 3.14 Konfigurasi <i>remote access</i> MongoDB	30
Gambar 3.15 <i>Structure document</i> <i>dionaea_raw_data</i>	30
Gambar 3.16 <i>Structure document</i> <i>client_hash_collection</i>	31
Gambar 3.17 Instalasi yara python	32
Gambar 3.18 <i>Deployment</i> modul collector	32
Gambar 3.19 <i>Install agent</i>	33
Gambar 3.20 <i>Method upload file using REST API</i>	33
Gambar 3.21 <i>Method malware identification</i>	34
Gambar 3.22 <i>Deployment</i> server deteksi	34
Gambar 3.23 <i>Flowchart</i> pengujian <i>collecting honeypot data</i>	35
Gambar 3.24 <i>Flowchart</i> pengujian <i>collecting hash client file</i>	36
Gambar 3.25 <i>Flowchart</i> pengujian <i>top-down malware detection</i>	37
Gambar 4.1 <i>Logs</i> harvester	39
Gambar 4.2 MQTT explorer	40
Gambar 4.3 <i>Logs</i> collector	40
Gambar 4.4 <i>Document</i> serangan dari <i>dionaea</i>	41
Gambar 4.5 <i>Logs created file agent</i>	43
Gambar 4.6 <i>Logs deleted file agent</i>	43
Gambar 4.7 <i>Document hash client file</i>	44
Gambar 4.8 <i>Log agent</i> ketika pendeteksian <i>malware</i>	45
Gambar 4.9 Hasil yara <i>scan malware types</i>	46
Gambar 4.10 <i>Logs</i> pengujian <i>offline client</i>	51



DAFTAR TABEL

Tabel 2.1 Ringkasan acuan penelitian	5
Tabel 3.1 Spesifikasi VPS	15
Tabel 3.2 Spesifikasi Laptop pengembangan sistem	16
Tabel 3.3 <i>Message</i> dan <i>Topic</i> yang digunakan	26
Tabel 4.1 Hasil pengujian <i>collecting data honeypot</i>	42
Tabel 4.2 Hasil pengujian <i>collecting client hash file</i>	44
Tabel 4.3 Hasil pengujian <i>top-down malware detection</i>	46
Tabel 4.4 Hasil pengujian akurasi pendeteksian <i>malware</i>	47
Tabel 4.5 <i>Multi client with malware 6567e663303386b7152d5fcab1f06cac</i>	48
Tabel 4.6 <i>Multi client with malware 996c2b2ca30180129c69352a3a3515e4</i>	49
Tabel 4.7 <i>Multi client with malware 85045b5163dc9ac209b946d2eace2bd8</i>	49
Tabel 4.8 Pengujian <i>client offline</i>	50



DAFTAR LAMPIRAN

Lampiran 1 Kode <i>agent</i>	56
Lampiran 2 Kode <i>Server Detection</i>	62
Lampiran 3 Dockerfile <i>server detection</i>	70
Lampiran 4 <i>File</i> konfigurasi harvester	71
Lampiran 5 <i>File service</i> harvester	71
Lampiran 6 <i>File</i> kode harvester	72
Lampiran 7 <i>File service</i> collector	90
Lampiran 8 <i>File service</i> collector	91
Lampiran 9 <i>File</i> kode collector	91
Lampiran 10 Contoh yara rule	93