

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xvi
INTISARI.....	xvii
<i>ABSTRACT</i>	xviii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	7
C. Batasan Masalah	7
D. Tujuan Penelitian	8
E. Manfaat Penelitian	9
BAB II TINJAUAN PUSTAKA.....	10
A. Landasan Teori.....	10
B. Penelitian Sebelumnya.....	38
BAB III METODE PENELITIAN.....	47
A. Waktu Penelitian.....	47
B. Metode Pengumpulan Data.....	47
C. Alat dan Bahan Penelitian.....	49
D. Konsep Penelitian	50

BAB IV HASIL DAN PEMBAHASAN	59
A. <i>Prepare</i> (Persiapan)	59
B. <i>Plan</i> (Perencanaan)	62
C. <i>Design</i> (Perancangan)	64
D. <i>Implement</i> (Implementasi)	66
E. <i>Operate</i> (Operasional)	81
F. <i>Optimize</i> (Optimasi).....	85
G. Hasil Analisis	86
BAB V PENUTUP.....	100
A. Kesimpulan	100
B. Saran	101
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR TABEL

Tabel 2.1 Penelitian Sebelumnya	43
Tabel 4.1 Spesifikasi VM (Integrasi YARA Rules).....	62
Tabel 4.2 Spesifikasi VM (Integrasi VirusTotal).....	63
Tabel 4.3 Spesifikasi VM <i>Attacker</i>	63
Tabel 4.4 Hasil Akurasi Deteksi	90
Tabel 4.5 Waktu Respon Deteksi ubuntu-yara-endpoint	91
Tabel 4.6 Waktu Respon Deteksi windows-yara-endpoint.....	92
Tabel 4.7 Waktu Respon Deteksi ubuntu-vt-endpoint.....	93
Tabel 4.8 Waktu Respon Deteksi windows-vt-endpoint.....	94
Tabel 4.9 Rata-rata Waktu Respons Deteksi.....	94
Tabel 4.10 Penggunaan <i>Resource</i> (Sumber Daya Sistem).....	97
Tabel 4.11 Perbandingan Kinerja Integrasi YARA Rules dan VirusTotal	98

DAFTAR GAMBAR

Gambar 2.1 Tampilan <i>Desktop</i> pada <i>Device</i> yang Terkena Lockbit 3.0	16
Gambar 2.2 File Terenkripsi Lockbit 3.0.....	17
Gambar 2.3 Lockbit 3.0 <i>Ransom Note</i>	18
Gambar 2.4 Situs <i>Data Leak</i> Lockbit 3.0.....	19
Gambar 2.5 Arsitektur Wazuh	25
Gambar 2.6 Arsitektur <i>Hypervisor Type 1</i>	34
Gambar 2.7 Contoh <i>Hypervisor Type 1</i>	35
Gambar 2.8 Arsitektur <i>Hypervisor Type 2</i>	36
Gambar 2.9 Contoh <i>Hypervisor Type 2</i>	37
Gambar 3.1 Kerangka Penelitian	51
Gambar 3.2 Metode Pengembangan PPDIIO.....	53
Gambar 4.1 Topologi Jaringan.....	65
Gambar 4.2 Proses Pengunduhan YARA <i>Detection Rules (Endpoint Ubuntu)</i>	67
Gambar 4.3 <i>Script yara.sh</i> untuk <i>Active Response</i>	67
Gambar 4.4 Konfigurasi Monitoring Direktori YARA pada Ubuntu.....	68
Gambar 4.5 <i>Script</i> download_yara_rules.py	68
Gambar 4.6 Proses Pengunduhan YARA <i>Detection Rules (Endpoint Windows)</i> 69	
Gambar 4.7 <i>Script yara.bat</i> untuk <i>Active Response</i>	69
Gambar 4.8 Konfigurasi Monitoring Direktori YARA pada Windows.....	70
Gambar 4.9 Konfigurasi Monitoring Direktori VirusTotal pada Ubuntu.....	70
Gambar 4.10 <i>Script</i> remove-threat.sh untuk <i>Active Response</i>	71
Gambar 4.11 Konfigurasi Monitoring Direktori VirusTotal pada Windows.....	71
Gambar 4.12 <i>Script</i> remove-threat.py untuk <i>Active Response</i>	72
Gambar 4.13 Konversi <i>Script</i> remove-threat.py menjadi .exe.....	73
Gambar 4.14 Konfigurasi local_rules.xml YARA (Ubuntu)	74
Gambar 4.15 Konfigurasi local_rules.xml YARA (Windows).....	74
Gambar 4.16 Konfigurasi local_decoder.xml Integrasi YARA.....	75
Gambar 4.17 Konfigurasi ossec.conf YARA (Ubuntu)	75
Gambar 4.18 Konfigurasi ossec.conf YARA (Windows).....	76

Gambar 4.19 Tampilan API Key pada Platform VirusTotal	76
Gambar 4.20 Konfigurasi ossec.conf VirusTotal (Ubuntu)	77
Gambar 4.21 Konfigurasi ossec.conf VirusTotal (Windows)	77
Gambar 4.22 Konfigurasi local_rules.xml VirusTotal (Ubuntu)	78
Gambar 4.23 Konfigurasi local_rules.xml VirusTotal (Windows)	78
Gambar 4.24 Struktur File <i>Ransomware</i> LockBit 3.0 <i>Builder</i>	79
Gambar 4.25 Proses Kompilasi <i>Ransomware</i> LockBit 3.0	79
Gambar 4.26 Struktur Direktori <i>Build Ransomware</i> LockBit 3.0	80
Gambar 4.27 Hasil <i>Build Ransomware</i> LockBit 3.0 Sebanyak 4 File	80
Gambar 4.28 Pengiriman <i>Ransomware</i> ke lockbit-srv via SCP	81
Gambar 4.29 Distribusi <i>Ransomware</i> melalui <i>Web Server</i> pada lockbit-srv	81
Gambar 4.30 <i>Script</i> ransom.sh	82
Gambar 4.31 <i>Output Script</i> ransom.sh	83
Gambar 4.32 <i>Script</i> ransom.bat	84
Gambar 4.33 <i>Output Script</i> ransom.bat	84
Gambar 4.34 Pengelompokkan VM di VMware Workstation Pro	85
Gambar 4.35 <i>Log</i> YARA Rules dari ubuntu-yara-endpoint	87
Gambar 4.36 <i>Log</i> YARA Rules dari windows-yara-endpoint	87
Gambar 4.37 <i>Log</i> VirusTotal dari ubuntu-vt-endpoint	88
Gambar 4.38 <i>Log</i> VirusTotal dari windows-vt-endpoint	89
Gambar 4.39 Penggunaan CPU <i>Server</i> wazuh-yara	95
Gambar 4.40 Penggunaan <i>Memory Server</i> wazuh-vt	96
Gambar 4.41 Penggunaan CPU <i>Server</i> wazuh-vt	96
Gambar 4.42 Penggunaan <i>Memory Server</i> wazuh-vt	96

DAFTAR LAMPIRAN

- Lampiran 1. Kartu Bimbingan Skripsi Pembimbing 1
- Lampiran 2. Kartu Bimbingan Skripsi Pembimbing 2
- Lampiran 3. *Log* JSON Hasil Deteksi
- Lampiran 4. Data Perhitungan Akurasi Deteksi (*Detection Accuracy*)
- Lampiran 5. Data Perhitungan Waktu Respons (*Response Time*)

