

DAFTAR ISI

LEMBAR PERNYATAAN ORISINAL.....	iii
ABSTRAK.....	iv
ABSTRACT	v
KATA PENGANTAR	vi
LEMBAR PERSEMBAHAN.....	vii
DAFTAR ISI	xxi
DAFTAR GAMBAR.....	xv
DAFTAR TABEL	xxi
DAFTAR LAMPIRAN	xxi
DAFTAR SINGKATAN.....	xxiii
DAFTAR ISTILAH.....	xxiv
BAB I PENDAHULUAN.....	1
I.1. Latar Belakang.....	1
I.2. Perumusan Masalah.....	4
I.3. Tujuan Penelitian	4
I.4. Manfaat Penelitian.....	4
I.5. Batasan Masalah	5
I.6. Sistematika Penelitian.....	5
BAB II TINJAUAN PUSTAKA	8
II.1. <i>Vulnerability</i>	8

II.2.	Teknologi <i>Container</i>	8
II.2.1.	Definisi Docker.....	8
II.2.2.	Komponen Docker.....	9
II.3.	<i>Content Management System (CMS)</i>	10
II.3.1.	Joomla.....	10
II.4.	<i>Vulnerability Scanning</i>	11
II.4.1.	Aquasec	11
II.4.2.	Anchore	12
II.5.	Teknologi Virtualisasi	14
II.6.	<i>Tools</i> Pengujian	14
II.7.	<i>Common Vulnerability Scoring System (CVSS)</i>	14
II.7.1.	Definisi CVSS	14
II.7.2.	<i>Base Container Metrics</i>	15
II.7.3.	<i>Temporal Container Metrics</i>	16
II.7.4.	<i>Environmental Container Metrics</i>	17
II.7.5.	Kalkulator CVSS v.3.1	17
II.8.	NVD NIST.....	17
II.8.1.	Definisi	17
II.8.2.	Kalkulator CVSS v.3.1 pada NVD.....	17
II.9.	Analisa Statistik Deskriptif.....	18
II.10.	<i>Cybersecurity Framework</i>	18
II.11.	<i>Cyber Resilience Review (CRR)</i>	18
II.11.1.	Definisi	18
II.11.2.	<i>Vulnerability Management</i> berdasarkan <i>Cyber Resilience Review</i> (CRR) 20	
II.12.	Penelitian Terdahulu.....	27
II.13.	Penelitian Terkini/Saat Ini	28

BAB III METODOLOGI PENELITIAN	30
III.1. Kerangka Pemecahan Masalah / Pengembangan Model Konseptual.....	30
III.2. Sistematika Penyelesaian Masalah	31
III.3.1. Tahap Hipotesis	33
III.3.2. Tahap <i>Design Platform</i> Pengujian.....	34
III.3.3. Tahap Implementasi	34
III.3.4. Tahap Analisis	34
III.3.5. Tahap Akhir	35
BAB IV RANCANGAN PENGUJIAN	37
IV.1.1. Identifikasi <i>Standard Remediation Timelines</i>	37
IV.1.2. Identifikasi <i>Periodic Activities</i>	37
IV.2. Identifikasi <i>Tools</i>	38
IV.2.1. Spesifikasi Perangkat Keras	38
IV.2.2. Spesifikasi Perangkat Lunak	39
IV.3. Topologi.....	47
IV.4. Skenario Pengujian	48
IV.4.1. Skenario <i>Vulnerability Scanning</i>	48
IV.4.2. Skenario Identifikasi <i>Category</i> dan <i>Priorotize</i>	49
IV.5. Identifikasi <i>Sources of Vulnerabilities Information</i>	52
BAB V IMPLEMENTASI DAN HASIL PENGUJIAN	53
V.1. <i>Record Periodic Activities</i>	53
V.1.1. Bulan Pertama.....	53
V.1.2. Bulan Kedua	54
V.2. <i>Record Discovered Vulnerabilities</i>	55
V.2.1. Pengujian Aquasec	55
V.2.2. Pengujian Anchore	66
BAB VI ANALISIS HASIL PENGUJIAN.....	75

VI.1. <i>Time Detection</i>	75
VI.2. <i>Vulnerability Evaluation</i>	76
VI.2.1. Data Perubahan Total <i>Vulnerabilities</i> Bulan Pertama dan Bulan Kedua 76	
VI.2.2. Data Perubahan Total <i>Vulnerabilities</i> pada Versi Lama dan Versi Baru pada Bulan Kedua.....	79
VI.2.3. Data Perbandingan Aquasec dan Anchore berdasarkan Total <i>Vulnerabilities</i> Setiap Versi.....	81
VI.2.4. Data Perbandingan Aquasec dan Anchore berdasarkan <i>Operating System Support</i>	83
VI.2.5. Data perbandingan Aquasec dan Anchore berdasarkan <i>Time for Detection</i> 84	
VI.3. <i>Categorize and Prioritize Vulnerabilities</i>	86
VI.3.1. Data Docker Berdasarkan Pengujian Aquasec	87
VI.3.2. Data Docker berdasarkan Anchore	92
VI.3.3. Data Joomla berdasarkan Aquasec	95
VI.3.4. Data Joomla berdasarkan Anchore	103
VI.4. Identifikasi <i>Vulnerability Patch</i> dan <i>Time for Remediation</i>	113
VI.4.1. Data Docker berdasarkan Aquasec	114
VI.4.2. Data Docker berdasarkan Anchore	114
VI.4.3. Data Joomla berdasarkan Aquasec	115
VI.4.4. Data Joomla berdasarkan Anchore	116
VI.5. Identifikasi <i>Root Causes</i>	119
BAB VII KESIMPULAN DAN SARAN	125
VII.1. KESIMPULAN	125
VII.2. SARAN.....	126
DAFTAR PUSTAKA.....	127
DAFTAR LAMPIRAN	131

Lampiran 1. <i>Vulnerability Report</i>	131
Lampiran 2. <i>Pull Aset IT</i>	132
Lampiran 3. Instalasi <i>tools</i> dan penggunaan	132
Lampiran 4. Proses Pengujian	134
Lampiran 5. Perhitungan CVSS <i>Base Vector</i>	143