

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR ORISINALITAS	iii
ABSTRAK.....	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABLE	xi
BAB 1 PENDAHULUAN.....	12
1.1. Latar Belakang	12
1.2. Rumusan Masalah	13
1.3. Tujuan dan Manfaat.....	13
1.4. Batasan Masalah	14
1.5. Metode Penelitian	15
BAB 2 TINJAUAN PUSTAKA.....	17
2.1. Tinjauan Pustaka	17
2.2. Landasan Teori	29
2.2.1. Docker Container	29
2.2.2. OpenVAS	29
2.2.3. Docker Scout	30
2.2.4. Standar PTES (Penetration Testing Execution Standart).....	30
2.2.5. Kerentanan Sistem (System Vulnerabilities)	30
2.2.6. SQL Injection	30
2.2.7. Flowchart.....	31
BAB 3 PERANCANGAN SISTEM	32
3.1. Subjek dan Objek Penelitian.....	32
3.2. Alat dan Bahan Penelitian	32
3.3. Topologi Perancangan.....	34
3.4. Diagram Alir Penelitian	35
3.4.1. Persiapan Lingkungan	37
3.4.2. Memasukan Target Pemindaian	37

3.4.3.	Pemindaian Kerentanan	38
3.4.4.	Output Scanning	38
3.4.5.	Analisis Hasil	38
3.4.6.	Penyerangan : SQL Injection	38
3.4.7.	Analisis Pasca Penyerangan	39
3.5.	Metode Analisis Kerentanan PTES	39
3.5.1.	Pre-engagement Interactions	41
3.5.2.	Intelligence Gathering	42
3.5.3.	Threat Modeling	42
3.5.5.	Exploitation	42
3.5.6.	Post Exploitation	43
3.5.7.	Reporting	43
BAB 4	HASIL PERCOBAAN DAN ANALISIS	44
4.1.	Proses Scan Vulnerability Docker Image Dengan Openvas	44
4.1.1.	Pre-engagement Interactions	44
4.1.2.	Intelligence Gathering	45
4.1.3.	Threat Modeling	46
4.1.4.	Reporting Scan Vulnerability Dengan OpenVAS	52
4.2.	Proses Scan Vulnerability Docker Image Dengan Docker Scout ..	57
4.2.1.	Pre-engagement Interactions	59
4.2.2.	Intelligence Gathering	59
4.2.3.	Threat Modeling	60
4.2.4.	Reporting Scan Vulnerability Dengan Docker Scout	62
4.3.	Perbedaan Scan Vulnerability OpenVAS dan Docker Scout	63
4.4.	Exploitation	65
4.5.	Post Exploitation	67
4.6.	Reporting	68
4.5.1.	Risiko	68
4.5.2.	Mitigasi	69
BAB 5	KESIMPULAN DAN SARAN	70
5.1.	Kesimpulan	70
5.2.	Saran	70
DAFTAR PUSTAKA		72