

DAFTAR ISI

ABSTRAK	ii
<i>ABSTRACT</i>	iii
LEMBAR PENGESAHAN	iv
LEMBAR PERNYATAAN ORISINALITAS	v
KATA PENGANTAR	vi
LEMBAR PERSEMBAHAN	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
DAFTAR SINGKATAN	xiv
DAFTAR ISTILAH	xv
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan Penelitian	2
I.4 Batasan Penelitian	2
I.5 Manfaat Penelitian	3
I.6 Sistematika Penulisan	3
BAB II LANDASAN TEORI	6
II.1 <i>Open-Source Intelligence</i> (OSINT)	6
II.2 Data Publik	6
II.3 <i>Reconnaissance</i>	6
II.4 Profil Risiko	7
II.5 <i>Framework Profiling</i> Risiko	7
II.5.1 <i>Threat</i> (T)	8
II.5.2 <i>Vulnerability</i> (V)	8
II.5.3 <i>Asset</i> (A)	8
II.6 <i>Threat Modelling</i>	9

II.7	<i>Data Flow Diagram</i>	9
II.8	<i>Attack Tree</i>	10
II.9	Alasan Pemilihan Kerangka Kerja	11
II.10	Penelitian Terdahulu.....	12
BAB III METODOLOGI PENELITIAN.....		15
III.1	Model Konseptual	15
III.2	Sistematika Penyelesaian Masalah.....	16
III.2.1	Tahap Awal.....	17
III.2.2	Tahap Hipotesis.....	17
III.2.3	Tahap Desain.....	18
III.2.4	Tahap Eksperimen.....	18
III.2.5	Tahap Analisis	18
III.2.6	Tahap Akhir.....	19
III.3	Pengumpulan Data	19
III.4	Pengolahan Data.....	20
III.5	Metode Evaluasi.....	20
BAB IV EKSPERIMEN DAN DATA		21
IV.1	Sumber Data.....	21
IV.2	Data Berdasarkan <i>Review</i> Literatur.....	22
IV.3	Perencanaan dan Persiapan Eksperimen	23
IV.3.1	Spesifikasi Perangkat Keras.....	23
IV.3.2	Spesifikasi Perangkat Lunak.....	24
IV.4	Alur Eksperimen	26
IV.4.1	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Berbasis CLI	27
IV.4.2	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Berbasis <i>Web</i>	28
IV.4.3	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Berbasis Ekstensi Peramban.....	29
IV.5	Implementasi Eksperimen.....	30
IV.5.1	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> whois	30
IV.5.2	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> nslookup ...	31
IV.5.3	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> amass	32

IV.5.4 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> theHarvester	33
IV.5.5 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> curl.....	34
IV.5.6 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> nmap	35
IV.5.7 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> dmitry	36
IV.5.8 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> sslscan.....	37
IV.5.9 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Shodan	38
IV.5.10 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> REDbot.....	39
IV.5.11 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Wappalyzer	40
IV.6 Data Hasil Eksperimen.....	41
BAB V ANALISIS.....	47
V.1 Perumusan Nilai <i>Asset</i> (A).....	47
V.2 Perumusan Nilai <i>Vulnerability</i> (V).....	49
V.3 Perumusan Nilai <i>Threat</i> (T)	60
V.4 Pemetaan Skenario Ancaman	67
V.4.1 Model Serangan: <i>Credential Sniffing</i> dari Protokol Tanpa Enkripsi	68
V.4.2 Model Serangan: <i>Remote Code Execution</i> (RCE)	70
V.4.3 Model Serangan: <i>Cloud Misconfiguration</i>	73
V.5 Perhitungan Nilai Risiko (R).....	75
V.6 Analisis Perbandingan Nilai Risiko	78
V.7 Ringkasan Analisis	81
BAB VI KESIMPULAN DAN SARAN	83
VI.1 Kesimpulan	83
VI.2 Saran.....	84
DAFTAR PUSTAKA	85