

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	x
DAFTAR LAMPIRAN.....	xi
DAFTAR SINGKATAN	xiii
DAFTAR ISTILAH	xiv
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan Penelitian	2
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian	3
I.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	7
II.1 Data Publik.....	7
II.2 <i>Risk Assestment</i>	7
II.3 <i>Open-Source Intelligence</i> (OSINT)	7
II.4 <i>Information Gathering</i>	8
II.5 <i>Cyber profiling</i>	8
II.6 <i>Threat Modeling</i>	9
II.7 <i>Asset IT</i>	9
II.8 Ancaman Siber	9
II.9 Alasan Pemilihan Kerangka Kerja	10
II.10 Penelitian Terdahulu	10
BAB III METODOLOGI PENELITIAN.....	13
III.1 Metode Konseptual	13
III.2 Sistematika Penyelesaian Masalah.....	14

III.2.1	Tahap Awal	15
III.2.2	Tahap Hipotesis	16
III.2.3	Tahap Perencanaan	16
III.2.4	Tahap Eksperimen	16
III.2.5	Tahap Analisis.....	17
III.2.6	Tahap Akhir	17
III.3	Pengumpulan Data	17
III.4	Pengolahan Data.....	18
III.5	Metode Evaluasi.....	19
BAB IV EKSPERIMEN DAN DATA		20
IV.1	Data Berdasarkan <i>Review</i> Literatur.....	20
IV.2	Perencanaan dan Persiapan Eksperimen	21
IV.2.1	Spesifikasi Perangkat Keras	21
IV.2.2	Spesifikasi Perangkat Lunak	22
IV.2.3	Daftar Target <i>Domain</i>	24
IV.3	Alur Eksperimen	25
IV.3.1	Alur Eksperimen Menggunakan OSINT <i>Tools</i> Berbasis CLI.....	25
IV.3.2	Alur Eksperimen Menggunakan OSINT <i>Tools</i> Berbasis <i>Website</i> ..	26
IV.3.3	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Berbasis <i>Extension</i> ..	27
IV.4	Implementasi Eksperimen.....	28
IV.4.1	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> whois	29
IV.4.2	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> nslookup ..	30
IV.4.3	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Shodan	31
IV.4.4	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> curl	32
IV.4.5	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Wappalyzer	33
IV.4.6	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> nmap	34
IV.4.7	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> sslscan.....	36
IV.4.8	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> REDbot....	38
IV.4.9	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> sublist3r ...	39
IV.4.10	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Traceroute	41
IV.4.11	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> dirb.....	42
IV.5	Ringkasan Data Eksperimen	43
BAB V ANALISIS		51
V.1	Perumusan Definisi <i>Asset</i> Information Technology (IT).....	51
V.2	Perumusan Nilai <i>Asset</i> (A).....	51

V.3	Perumusan Nilai <i>Vulnerability</i> (V)	53
V.4	Perumusan Nilai <i>Threat</i> (T)	56
V.5	Pemetaan Skenario Ancaman.....	62
V.5.1	Model Serangan <i>Credential Stuffing</i>	63
V.5.2	Model Serangan <i>Bruteforce Login</i>	66
V.5.3	Model Serangan <i>Man-in-the-Middle</i> (MitM).....	68
V.6	Perhitungan Nilai Risiko (R).....	71
V.7	Analisis Perbandingan Nilai Resiko (R) Pada IKS	73
V.8	Ringkasan Analisis.....	75
BAB VI KESIMPULAN DAN SARAN		79
VI.1	Kesimpulan	79
VI.2	Saran.....	81
DAFTAR PUSTAKA		82
LAMPIRAN.....		85