

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
Kata Pengantar	vi
Lembar Persembahan	vii
Daftar Isi.....	viii
Daftar Gambar.....	xii
Daftar Tabel	xiv
Daftar Lampiran	xv
Daftar Singkatan.....	xvi
Daftar Istilah.....	xvii
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.....	2
Bab II TINJAUAN PUSTAKA.....	4
II.1 <i>Open Source Intelligence (OSINT)</i>	4
II.2 Kali Linux.....	4
II.3 <i>Phishing</i>	4
II.4 <i>Social Engineering</i>	4
II.5 <i>Data Flow Diagram</i>	5
II.6 <i>Activity Diagram</i>	5

II.7	<i>Flowchart</i>	5
II.8	<i>Spear Phishing</i>	5
II.9	Mitigasi.....	5
II.10	Filter <i>Email</i>	6
II.11	<i>Technology Based</i>	6
II.12	Penelitian Terdahulu.....	7
Bab III	METODOLOGI PENELITIAN	8
III.1	Model Konseptual	8
III.2	Sistematika Penyelesaian Masalah.....	9
III.2.1	Tahap Awal	11
III.2.2	Hipotesa.....	11
III.2.3	Tahap Eksperimen.....	11
III.2.4	Tahap Analisis.....	11
III.2.5	Tahap Pelaporan.....	12
III.3	Pengumpulan Data	12
III.4	Pengolahan Data.....	12
III.5	Metode Evaluasi	12
Bab IV	EKSPERIMEN DAN DATA	13
IV.1	Spesifikasi Perangkat	13
IV.1.1	Spesifikasi Perangkat Keras.....	13
IV.1.2	Spesifikasi Perangkat Lunak.....	14
IV.1.3	Skenario Pengerjaan.....	16
IV.2	Implementasi Eksperimen	22
IV.2.1	Implementasi Eksperimen TheHarvester Terhadap Data <i>Input</i> dan <i>Output</i>	22

IV.2.2	Implementasi Eksperimen Spiderfoot Terhadap Data <i>Input</i> dan <i>Output</i>	24
IV.2.3	Implementasi Eksperimen Skymem Terhadap Data <i>Input</i> dan <i>Output</i>	25
IV.2.4	Implementasi Eksperimen GoogleFU Terhadap Data <i>Input</i> dan <i>Output</i>	26
IV.2.5	Implementasi Eksperimen SEToolkit Terhadap Data <i>Input</i> dan <i>Output</i>	28
IV.2.6	Implementasi Eksperimen <i>Phishing Attack</i> Dengan SEToolkit Berdasarkan Konten <i>Email</i>	29
IV.3	Data Eksperimen	32
IV.3.1	Data Eksperimen Menggunakan TheHarvester	33
IV.3.2	Data Eksperimen Menggunakan Spiderfoot	35
IV.3.3	Data Eksperimen Menggunakan Skymem	36
IV.3.4	Data Eksperimen Menggunakan GoogleFU	37
IV.3.5	Data Eksperimen Menggunakan SEToolkit.....	38
Bab V	ANALISIS	39
V.1	Implementasi <i>Tools</i> Berdasarkan <i>Data Flow Diagram</i>	39
V.1.1	Hasil Implementasi Data Flow Terhadap TheHarvester	39
V.1.2	Hasil Implementasi Data Flow Terhadap Spiderfoot.....	40
V.1.3	Hasil Implementasi Data Flow Terhadap Skymem	42
V.1.4	Hasil Implementasi Data Flow Terhadap GoogleFu.....	43
V.1.5	Hasil Implementasi Data Flow Terhadap SEToolkit	44
V.2	Proses <i>Phishing Attack</i> Dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i>	46
V.2.1	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> Terhadap <i>Website</i> 1 Divisi PT. XYZ.....	47

V.2.2	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> Terhadap <i>Website 2</i> Divisi PT. XYZ.....	49
V.3	<i>Analisa Phishing Attack</i>	51
V.3.1	Tabel Perbandingan Terhadap Konten <i>Email</i>	51
V.3.2	Aspek <i>People, Process & Technology</i> Berdasarkan Hasil Eksperimen	52
V.3.3	Mitigasi <i>Phishing Attack</i> Berdasarkan Metode <i>Technology Based</i>	55
Bab VI	KESIMPULAN DAN SARAN	64
VI.1	Kesimpulan.....	64
VI.2	Saran	65
	Daftar Pustaka	66
	LAMPIRAN	68