

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>Flowchart</i>	5

II.6	<i>Activity Diagram</i>	5
II.7	<i>Data Flow Diagram (DFD)</i>	5
II.8	<i>Spear Phishing</i>	5
II.9	Mitigasi	5
II.10	<i>Auditing and Policy Based</i>	6
II.11	<i>Continuous Auditing</i>	6
II.12	<i>Standard Operating Procedure (SOP)</i>	6
II.13	Penelitian Terdahulu	6
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	Tahap 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.....	23

IV.2.1	Implementasi Eksperimen Aquatone Terhadap Data <i>Input</i> dan <i>Output</i>	23
IV.2.2	Implementasi Eksperimen Sublist3r Terhadap Data <i>Input</i> dan <i>Output</i>	25
IV.2.3	Implementasi Eksperimen Pentest- <i>tools</i> Terhadap Data <i>Input</i> dan <i>Output</i>	26
IV.2.4	Implementasi Eksperimen SynapsInt Terhadap Data <i>Input</i> dan <i>Output</i>	27
IV.2.5	Implementasi Eksperimen PhoneBook Terhadap Data <i>Input</i> dan <i>Output</i>	29
IV.2.6	Implementasi Eksperimen <i>Phishing</i> menggunakan Setoolkit Terhadap Data <i>Input</i> dan <i>Output</i>	30
IV.2.7	Implementasi Eksperimen <i>Phishing Attack</i> dengan SEToolkit berdasarkan Konten <i>Email</i>	32
IV.3	Data Eksperimen	35
IV.3.1	Data Eksperimen Menggunakan Aquatone	35
IV.3.2	Data Eksperimen Menggunakan Sublist3r	35
IV.3.3	Data Eksperimen Menggunakan Pentest- <i>tools</i>	36
IV.3.4	Data Eksperimen Menggunakan SynapsInt	37
IV.3.5	Data Eksperimen Menggunakan Phonebook	38
IV.3.6	Data Eksperimen <i>Phishing</i> Menggunakan SEToolkit.....	39
Bab V	ANALISIS	41
V.1	Implementasi <i>Tools</i> berdasarkan <i>Data Flow Diagram</i>	41
V.1.1	Hasil Implementasi <i>Data Flow</i> terhadap Aquatone	41
V.1.2	Hasil Implementasi <i>Data Flow</i> terhadap Sublist3r	42
V.1.3	Hasil Implementasi <i>Data Flow</i> terhadap Pentest- <i>tools</i>	43
V.1.4	Hasil Implementasi <i>Data Flow</i> terhadap SynapsInt.....	44

V.1.5	Hasil Implementasi <i>Data Flow</i> terhadap Phonebook.....	45
V.1.6	Hasil Implementasi <i>Data Flow</i> terhadap SEToolkit	47
V.2	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i>	49
V.2.1	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> terhadap <i>Website 1</i> Divisi PT.XYZ	49
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	51
V.3	Analisa <i>Phishing Attack</i>	52
V.3.1	Tabel Perbandingan terhadap Konten <i>Email Phishing</i>	53
V.3.2	Aspek <i>People, Process & Technology</i> berdasarkan Tabel Perbandingan Konten <i>Email Phishing</i>	55
V.3.3	Mitigasi <i>Phishing Attack</i> berdasarkan metode <i>Auditing and Policy Based</i>	58
Bab VI	KESIMPULAN DAN SARAN.....	82
VI.1	KESIMPULAN.....	82
VI.2	SARAN	83
	DAFTAR PUSTAKA.....	84
	LAMPIRAN	86