

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
Kata Pengantar	vi
Lembar Persembahan	vii
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.....	3
Bab II TINJAUAN PUSTAKA.....	4
II.1 <i>Open Source Intelligence (OSINT)</i>	4
II.2 Kali Linux	4
II.3 <i>Social engineering</i>	4
II.4 <i>Data Flow Diagram (DFD)</i>	4
II.5 <i>Activity Diagram</i>	5
II.6 <i>Flowchart</i>	5

II.7	<i>Phishing Attack</i>	5
II.8	<i>Spear Phishing</i>	5
II.9	<i>Social Media Phishing</i>	5
II.10	Mitigasi	6
II.11	<i>Human-Based</i>	6
II.12	Penelitian Terdahulu	7
Bab III	Metodologi Penelitian	9
III.1	Model Konseptual	9
III.2	Sistematika Penyelesaian Masalah	10
III.2.1	Tahap Awal	12
III.2.2	Tahap Hipotesa	12
III.2.3	Tahap Eksperimen	12
III.2.4	Tahap Analisis	12
III.2.5	Tahap Pelaporan	13
III.3	Metode Evaluasi	13
III.4	Alasan Pemilihan Metode	13
Bab IV	EKSPERIMEN DAN DATA	14
IV.1	Spesifikasi Perangkat	14
IV.1.1	Spesifikasi Perangkat Keras	14
IV.1.2	Spesifikasi Perangkat Lunak	15
IV.1.3	Skenario Pengerjaan	17
IV.2	Implementasi Eksperimen	25
IV.2.1	Implementasi Eksperimen Recon-NG Terhadap Data <i>Input</i> dan <i>Output</i>	25
IV.2.2	Implementasi Eksperimen Hunter Terhadap Data <i>Input</i> dan <i>Output</i>	27

IV.2.3	Implementasi Eksperimen Snov.io Terhadap Data <i>Input</i> dan <i>Output</i>	28
IV.2.4	Implementasi Eksperimen Get Prospect Terhadap Data <i>Input</i> dan <i>Output</i>	30
IV.2.5	Implementasi Eksperimen SEToolkit Terhadap Data <i>Input</i> dan <i>Output</i>	31
IV.2.6	Implementasi Eksperimen Zphisher Terhadap Data <i>Input</i> dan <i>Output</i>	32
IV.2.7	Implementasi Eksperimen <i>Phishing Attack</i> dengan SEToolkit berdasarkan Konten <i>Email</i>	34
IV.2.8	Implementasi Eksperimen <i>Phishing Attack</i> dengan Zphisher berdasarkan Konten <i>Email</i>	36
IV.3	Data Eksperimen	38
IV.3.1	Data Eksperimen menggunakan Recon-NG.....	39
IV.3.2	Data Eksperimen menggunakan Hunter	39
IV.3.3	Data Eksperimen menggunakan Snov.io.....	40
IV.3.4	Data Eksperimen menggunakan Get Prospect	41
IV.3.5	Data Eksperimen menggunakan SEToolkit.....	42
IV.3.6	Data Eksperimen menggunakan Zphisher.....	43
Bab V	ANALISIS	44
V.1	Implementasi <i>Tools</i> Berdasarkan <i>Data Flow Diagram</i> (DFD).....	44
V.1.1	Hasil Implementasi <i>Data Flow</i> terhadap Recon-NG.....	44
V.1.2	Hasil Implementasi <i>Data Flow</i> terhadap Hunter.....	45
V.1.3	Hasil Implementasi <i>Data Flow</i> terhadap Snov.io.....	46
V.1.4	Hasil Implementasi <i>Data Flow</i> terhadap Get Prospect	48
V.1.5	Hasil Implementasi <i>Data Flow</i> terhadap SEToolkit	49
V.1.6	Hasil Implementasi <i>Data Flow</i> terhadap Zphisher.....	51

V.2	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i>	52
V.2.1	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> terhadap Divisi 1 PT. XYZ.....	53
V.2.2	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> terhadap Divisi 2 PT. XYZ.....	54
V.2.3	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> terhadap Pegawai PT. XYZ (Facebook).....	56
V.2.4	Proses <i>Phishing Attack</i> dengan <i>Activity Diagram</i> Berdasarkan Konten <i>Email</i> terhadap Pegawai PT. XYZ (Instagram)	57
V.3	Analisa <i>Phishing Attack</i>	59
V.3.1	Tabel Perbandingan terhadap Konten <i>Email</i>	59
V.3.2	Aspek <i>People, Process & Technology</i> Berdasarkan Hasil Eksperimen	60
V.3.3	Mitigasi <i>Phishing Attack</i> Berdasarkan Metode <i>Human-Based</i> ...	64
V.3.3.1	Penanganan <i>Training and Awareness</i> Keamanan Informasi.....	64
V.3.3.2	Strategi Keberhasilan Pelatihan dan Kesadaran Pegawai	65
Bab VI	Kesimpulan dan Saran	75
VI.1	Kesimpulan.....	75
VI.2	Saran.....	76
	Daftar Pustaka	77
	LAMPIRAN.....	79