

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
LEMBAR PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xvii
DAFTAR LAMPIRAN	xix
DAFTAR ISTILAH	xx
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.....	3
Bab II TINJAUAN PUSTAKA.....	7
II.1 Landasan Teori	7
II.1.1 Data Publik.....	7
II.1.2 <i>Open-Source Intelligence</i> (OSINT)	7
II.1.3 <i>Threat</i>	8
II.1.4 <i>Cyber Security</i>	8
II.1.5 <i>Social Engineering</i>	8

II.1.6	<i>Phishing Attack</i>	9
II.1.7	<i>Quishing Attack</i>	9
II.1.8	<i>Quick Response (QR) Code</i>	10
II.1.9	<i>Metrik Cost</i>	10
II.1.10	<i>Threat Modeling</i>	10
II.1.11	<i>Attack Tree</i>	11
II.1.12	<i>Flowchart Diagram</i>	11
II.1.13	<i>Data Flow Diagram (DFD)</i>	12
II.2	Penelitian Terdahulu.....	14
II.3	Alasan Pemilihan Kerangka Kerja/Teori/Pendekatan	15
Bab III	METODOLOGI PENELITIAN	17
III.1	Model Konseptual.....	17
III.2	Sistematika Penyelesaian Masalah	18
III.2.1	Tahap Awal	20
III.2.2	Tahap Hipotesis.....	20
III.2.3	Tahap Desain.....	20
III.2.4	Tahap Eksperimen.....	20
III.2.5	Tahap Analisis.....	21
III.2.6	Tahap Akhir	21
III.3	Pengumpulan Data	21
III.4	Pengolahan Data	22
III.5	Metode Evaluasi	22
Bab IV	PERANCANGAN DAN ALUR EKSPERIMEN.....	23
IV.1	Perencanaan dan Persiapan Eksperimen.....	23
IV.1.1	Spesifikasi Perangkat Keras	23
IV.1.2	Spesifikasi Perangkat Lunak	24

IV.1.3	<i>Platform</i> Eksperimen	25
IV.1.4	Daftar IP <i>Address</i>	26
IV.2	Hasil Percobaan <i>Tools</i>	26
IV.3	Identifikasi Nomor Telepon Target melalui Media Sosial	28
IV.4	Alur Eksperimen	30
IV.4.1	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Truecaller	31
IV.4.2	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Sync.ME	33
IV.4.3	Alur Eksperimen Menggunakan <i>Social Engineering Tool</i> SEToolkit 35	
IV.4.4	Alur eksperimen Menggunakan <i>Social Engineering Tool</i> SocialFish 37	
IV.4.5	Alur Eksperimen Menggunakan QR Code <i>Tool</i> qrcode Berdasarkan <i>Phishing</i> URL SEToolkit.....	40
IV.4.6	Alur Eksperimen Menggunakan QR Code <i>Tool</i> qrcode Berdasarkan <i>Phishing</i> URL SocialFish	41
IV.4.7	Alur Eksperimen <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SEToolkit Melalui Konten Pesan <i>Phishing</i> di WhatsApp...	43
IV.4.8	Alur Eksperimen <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SocialFish Melalui Konten Pesan <i>Phishing</i> di WhatsApp ..	45
IV.5	Implementasi Eksperimen.....	47
IV.5.1	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Truecaller 48	
IV.5.2	Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Sync.ME	50
IV.5.3	Implementasi Eksperimen Menggunakan <i>Social Engineering Tool</i> SEToolkit.....	52
IV.5.4	Implementasi Eksperimen Menggunakan <i>Social Engineering Tool</i> SocialFish.....	56

IV.5.5	Implementasi Eksperimen Menggunakan QR Code Tool qrcode Berdasarkan <i>Phishing</i> URL SEToolkit.....	59
IV.5.6	Implementasi Eksperimen Menggunakan QR Code Tool qrcode Berdasarkan <i>Phishing</i> URL SocialFish	60
IV.5.7	Implementasi Eksperimen <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SEToolkit Melalui Konten Pesan <i>Phishing</i> di WhatsApp Terhadap Nasabah Bank XYZ.....	61
IV.5.8	Implementasi Eksperimen <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SocialFish Melalui Konten Pesan <i>Phishing</i> di WhatsApp Terhadap Nasabah Bank XYZ.....	64
IV.6	Data Hasil Eksperimen	67
IV.6.1	Data Hasil Eksperimen Menggunakan OSINT Tool Truecaller ...	67
IV.6.2	Data Hasil Eksperimen Menggunakan OSINT Tool Sync.ME.....	68
IV.6.3	Data Hasil Eksperimen Menggunakan <i>Social Engineering Tool</i> SEToolkit.....	68
IV.6.4	Data Hasil Eksperimen Menggunakan <i>Social Engineering Tool</i> SocialFish.....	69
IV.6.5	Data Hasil Eksperimen Menggunakan QR Code Tool qrcode Berdasarkan <i>Phishing</i> URL SEToolkit	69
IV.6.6	Data Hasil Eksperimen Menggunakan QR Code Tool qrcode Berdasarkan <i>Phishing</i> URL SocialFish.....	70
IV.6.7	Data Hasil Eksperimen <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SEToolkit Melalui Konten Pesan <i>Phishing</i> di WhatsApp Terhadap Nasabah Bank XYZ.....	71
IV.6.8	Data Hasil Eksperimen <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SocialFish Melalui Konten Pesan <i>Phishing</i> di WhatsApp Terhadap Nasabah Bank XYZ.....	72
Bab V	ANALISIS.....	74
V.1	Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan.....	74

V.1.1	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan OSINT Tool Truecaller	75
V.1.2	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan OSINT Tool Sync.ME	75
V.1.3	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan <i>Social Engineering Tool</i> SEToolkit	76
V.1.4	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan <i>Social Engineering Tool</i> SocialFish.....	78
V.1.5	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan QR Code Berisi <i>Phishing</i> URL SEToolkit dengan Tool qrencode	79
V.1.6	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan QR Code Berisi <i>Phishing</i> URL SocialFish dengan Tool qrencode	80
V.1.7	Hasil Perumusan <i>Data Flow Diagram</i> Untuk <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SEToolkit Melalui Konten Pesan <i>Phishing</i> di WhatsApp.....	81
V.1.8	Hasil Perumusan <i>Data Flow Diagram</i> Untuk <i>Quishing Attack</i> Menggunakan QR Code Berisi <i>Phishing</i> URL SocialFish Melalui Konten Pesan <i>Phishing</i> di WhatsApp.....	83
V.2	Perumusan <i>Data Flow Diagram</i> dari <i>Quishing Attack</i> Berdasarkan Serangan OSINT, <i>Social Engineering</i> , dan QR Code.....	84
V.2.1	Hasil Perumusan <i>Data Flow Diagram</i> dari <i>Quishing Attack</i> Berdasarkan Serangan OSINT Truecaller, <i>Social Engineering</i> SEToolkit, dan QR Code qrencode Melalui Konten Pesan <i>Phishing</i> di WhatsApp.....	85
V.2.2	Hasil Perumusan <i>Data Flow Diagram</i> dari <i>Quishing Attack</i> Berdasarkan Serangan OSINT Sync.ME, <i>Social Engineering</i> SocialFish dan QR Code qrencode Melalui Konten Pesan <i>Phishing</i> di WhatsApp.....	89
V.3	Analisis <i>Attack Tree</i>	94

V.4	Penyusunan <i>Attack Tree</i> Berdasarkan <i>Data Flow Diagram</i> dari <i>Quishing Attack</i>	94
V.4.1	Hasil Penyusunan <i>Attack Tree</i> Berdasarkan <i>Data Flow Diagram</i> Dari <i>Quishing Attack</i> Serangan OSINT Truecaller, <i>Social Engineering</i> SEToolkit, dan QR Code qrencode Melalui Konten Pesan <i>Phishing</i> di WhatsApp	95
V.4.2	Hasil Penyusunan <i>Attack Tree</i> Berdasarkan <i>Data Flow Diagram</i> Dari <i>Quishing Attack</i> Serangan OSINT Sync.ME, <i>Social Engineering</i> SocialFish, dan QR Code qrencode Melalui Konten Pesan <i>Phishing</i> Di WhatsApp	98
V.4.3	Hasil Penyusunan <i>Attack Tree</i> Berdasarkan <i>Data Flow Diagram</i> dari <i>Quishing Attack</i>	101
V.5	Pengukuran <i>Cost</i> pada <i>Quishing Attack</i>	103
V.5.1	Hasil Pengukuran <i>Cost</i> pada <i>Quishing Attack</i> Berdasarkan Serangan OSINT Truecaller, <i>Social Engineering</i> SEToolkit, dan QR Code Melalui Konten Pesan <i>Phishing</i> di WhatsApp	104
V.5.2	Hasil Pengukuran <i>Cost</i> pada <i>Quishing Attack</i> Berdasarkan Serangan OSINT Sync.ME, <i>Social Engineering</i> SocialFish, dan QR Code Melalui Konten Pesan <i>Phishing</i> di WhatsApp	105
V.6	Analisis Perbandingan Berdasarkan Metrik <i>Cost</i> pada <i>Quishing Attack</i>	107
V.7	Ringkasan Analisis	110
Bab VI	KESIMPULAN DAN SARAN	112
VI.1	Kesimpulan	112
VI.2	Saran	113
	DAFTAR PUSTAKA	114