

DAFTAR ISI

ABSTRAK	ii
<i>ABSTRACT</i>	iii
LEMBAR PENGESAHAN	iv
LEMBAR PERNYATAAN ORISINALITAS	v
KATA PENGANTAR	vi
LEMBAR PERSEMBAHAN	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xiv
DAFTAR TABEL.....	xvi
DAFTAR LAMPIRAN.....	xvii
DAFTAR SINGKATAN	xviii
DAFTAR ISTILAH	xix
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
I.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA	6
II.1 <i>Open Source Intelligence</i> (OSINT)	6
II.2 Data Publik	6
II.3 Ancaman (<i>Threat</i>)	7
II.4 Keamanan Siber (<i>Cyber Security</i>).....	7

II.5	<i>Social Engineering</i>	7
II.6	<i>Phishing Attack</i>	8
II.7	<i>Spear Phishing Attack</i>	8
II.8	<i>Email Spoofing</i>	9
II.9	Metrik Granularitas Data	9
II.10	<i>Attack Tree</i>	9
II.11	<i>Data Flow Diagram (DFD)</i>	10
II.12	Diagram Alur (<i>Flowchart</i>).....	10
II.13	<i>Mail Server</i>	10
II.14	Telnet	11
II.15	<i>Simple Mail Transfer Protocol (SMTP)</i>	11
II.16	Kali Linux	11
II.17	Penelitian Terdahulu	11
BAB III	METODOLOGI PENELITIAN	16
III.1	Model Konseptual.....	16
III.2	Sistematika Penyelesaian Masalah	17
III.2.1	Tahap Awal	19
III.2.2	Tahap Hipotesis.....	19
III.2.3	Tahap Desain.....	19
III.2.4	Tahap Eksperimen.....	19
III.2.5	Tahap Analisis.....	20
III.2.6	Tahap Akhir	20
III.3	Pengumpulan Data	20
III.4	Pengolahan Data	21
III.5	Metode Evaluasi	21
BAB IV	PERENCANAAN DAN ALUR EKSPERIMEN	22

IV.1	Perencanaan dan Persiapan	22
IV.1.1	Spesifikasi Perangkat Keras	22
IV.1.2	Spesifikasi Perangkat Lunak	22
IV.1.3	<i>Platform</i> Eksperimen	24
IV.1.4	Daftar <i>IP Address</i>	25
IV.2	Alur Eksperimen	26
IV.2.1	Alur Eksperimen Menggunakan OSINT <i>Tool</i> TheHarvester.....	26
IV.2.2	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Metagoofil.....	27
IV.2.3	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Recon-ng.....	29
IV.2.4	Alur Eksperimen Menggunakan OSINT <i>Tool</i> Snov.io	31
IV.2.5	Alur Eksperimen Menggunakan <i>Social Engineering Tool</i> SEToolkit	33
IV.2.6	Alur Eksperimen Menggunakan <i>Social Engineering Tool</i> Zphisher	35
IV.2.7	Alur Eksperimen <i>Email Spoofing</i> Menggunakan Telnet	37
IV.3	Implementasi Eksperimen.....	39
IV.3.1	Implementasi Eksperimen OSINT <i>Tool</i> TheHarvester	39
IV.3.2	Implementasi Eksperimen OSINT <i>Tool</i> Metagoofil.....	41
IV.3.3	Implementasi Eksperimen OSINT <i>Tool</i> Recon-ng	42
IV.3.4	Implementasi Eksperimen OSINT <i>Tool</i> Snov.io	43
IV.3.5	Implementasi Eksperimen <i>Social Engineering Tool</i> SEToolkit ...	44
IV.3.6	Implementasi Eksperimen <i>Social Engineering Tool</i> Zphisher.....	46
IV.3.7	Implementasi Eksperimen Pengiriman <i>Email Spoofing</i>	48
IV.4	Data Hasil Eksperimen	50
IV.4.1	Data Hasil Eksperimen OSINT <i>Tool</i> TheHarvester.....	50
IV.4.2	Data Hasil Eksperimen OSINT <i>Tool</i> Metagoofil.....	53

IV.4.3	Data Hasil Eksperimen OSINT <i>Tool Recon-ng</i>	54
IV.4.4	Data Hasil Eksperimen OSINT <i>Tool Snov.io</i>	57
IV.4.5	Data Hasil Eksperimen <i>Social Engineering Tool SEToolkit</i>	60
IV.4.6	Data Hasil Eksperimen <i>Social Engineering Tool Zphisher</i>	60
IV.4.7	Data Hasil Eksperimen Pengiriman <i>Email Spoofing</i>	60
BAB V	ANALISIS	62
V.1	Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan.....	62
V.1.1	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan OSINT <i>Tool TheHarvester</i>	62
V.1.2	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan OSINT <i>Tool Metagoofil</i>	63
V.1.3	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan OSINT <i>Tool Recon-ng</i>	64
V.1.4	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan OSINT <i>Tool Snov.io</i>	65
V.1.5	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan <i>Social Engineering Tool SEToolkit</i>	66
V.1.6	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan Menggunakan <i>Social Engineering Tool Zphisher</i>	68
V.1.7	Hasil Perumusan <i>Data Flow Diagram</i> Berdasarkan Serangan <i>Email Spoofing</i> Menggunakan Telnet	69
V.2	Perumusan <i>Data Flow Diagram</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT, <i>Social Engineering</i> , dan <i>Email Spoofing</i>	71
V.2.1	Hasil Perumusan <i>Data Flow Diagram</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT <i>TheHarvester</i> , <i>Social Engineering SEToolkit</i> , dan <i>Email Spoofing</i>	72

V.2.2	Hasil Perumusan <i>Data Flow Diagram</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Metagoofil, <i>Social Engineering Zphisher</i> , dan <i>Email Spoofing</i>	76
V.2.3	Hasil Perumusan <i>Data Flow Diagram</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Recon-ng, <i>Social Engineering SEToolkit</i> , dan <i>Email Spoofing</i>	79
V.2.4	Hasil Perumusan <i>Data Flow Diagram</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Snov.io, <i>Social Engineering Zphisher</i> , dan <i>Email Spoofing</i>	83
V.3	Analisis <i>Attack Tree</i> Berdasarkan <i>Data Flow Diagram Spear Phishing Attack</i>	87
V.3.1	<i>Attack Tree</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT TheHarvester, <i>Social Engineering SEToolkit</i> , dan <i>Email Spoofing</i>	88
V.3.2	<i>Attack Tree</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Metagoofil, <i>Social Engineering Zphisher</i> , dan <i>Email Spoofing</i>	91
V.3.3	<i>Attack Tree</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Recon-ng, <i>Social Engineering SEToolkit</i> , dan <i>Email Spoofing</i>	93
V.3.4	<i>Attack Tree</i> dari <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Snov.io, <i>Social Engineering Zphisher</i> , dan <i>Email Spoofing</i>	96
V.3.5	Hasil <i>Attack Tree</i> Berdasarkan <i>Spear Phishing Attack</i>	99
V.4	Pengukuran Granularitas Data Pada <i>Spear Phishing Attack</i>	101
V.4.1	Hasil Pengukuran Granularitas Data <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT TheHarvester, <i>Social Engineering SEToolkit</i> , dan <i>Email Spoofing</i>	102
V.4.2	Hasil Pengukuran Granularitas Data <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Metagoofil, <i>Social Engineering Zphisher</i> , dan <i>Email Spoofing</i>	102

V.4.3 Hasil Pengukuran Granularitas Data <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Recon-ng, <i>Social Engineering SEToolkit</i> , dan <i>Email Spoofing</i>	103
V.4.4 Hasil Pengukuran Granularitas Data <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Snov.io, <i>Social Engineering Zphisher</i> , dan <i>Email Spoofing</i>	104
V.5 Analisis Perbandingan <i>Attack Tree</i> Berdasarkan <i>Spear Phishing Attack</i> Dengan Metrik Granularitas Data	105
V.6 Ringkasan Analisis	109
BAB VI KESIMPULAN DAN SARAN	110
VI.1 Kesimpulan	110
VI.2 Saran	111
DAFTAR PUSTAKA	112