

DAFTAR GAMBAR

Gambar III.1 Model konseptual penelitian	12
Gambar III.2 Sistematika penyelesaian masalah	14
Gambar IV.1 Diagram platform eksperimen	20
Gambar IV.2 Alur eksperimen menggunakan OSINT <i>tool</i> Knockpy	21
Gambar IV.3 Alur eksperimen menggunakan OSINT <i>tool</i> Skymem	22
Gambar IV.4 Alur eksperimen menggunakan OSINT <i>tool</i> SpiderFoot.....	23
Gambar IV.5 Alur eksperimen menggunakan <i>social engineering tool</i> SEToolkit	24
Gambar IV.6 Alur eksperimen menggunakan <i>social engineering tool</i> Dark-Phish	25
Gambar IV.7 Alur eksperimen <i>email spoofing</i> menggunakan Telnet.....	26
Gambar IV.8 Mengakses dan menjalankan Knockpy	28
Gambar IV.9 Data hasil <i>scanning</i> menggunakan Knockpy	29
Gambar IV.10 Halaman utama <i>website</i> Skymem	29
Gambar IV.11 Hasil <i>scanning</i> menggunakan Skymem	30
Gambar IV.12 Mengakses dan menjalankan <i>web server</i> SpiderFoot	31
Gambar IV.13 Hasil <i>scanning</i> menggunakan SpiderFoot.....	32
Gambar IV.14 Menjalankan SEToolkit	33
Gambar IV.15 Hasil pembuatan <i>cloned website</i>	34
Gambar IV.16 Halaman utama <i>tool</i> Dark-Phish	34
Gambar IV.17 Proses serangan <i>email spoofing</i> menggunakan Telnet.....	35
Gambar IV.18 Penyerang berhasil mengirimkan <i>email</i> palsu	37
Gambar V.1 <i>Data flow diagram</i> serangan OSINT Knockpy	43
Gambar V.2 <i>Data flow diagram</i> serangan OSINT Skymem	44
Gambar V.3 <i>Data flow diagram</i> serangan OSINT SpiderFoot.....	45
Gambar V.4 <i>Data flow diagram</i> serangan <i>social engineering</i> SEToolkit	46
Gambar V.5 <i>Data flow diagram</i> serangan <i>social engineering</i> Dark-Phish	48
Gambar V.6 <i>Data flow diagram</i> serangan <i>email spoofing</i> Telnet	49
Gambar V.7 <i>Data flow diagram</i> dari <i>whaling attack</i> kombinasi serangan OSINT Knockpy, <i>social engineering</i> SEToolkit, dan <i>email spoofing</i> Telnet	52

Gambar V.8 <i>Data flow diagram</i> dari <i>whaling attack</i> kombinasi serangan OSINT Skymem, <i>social engineering</i> Dark-Phish, dan <i>email spoofing</i> Telnet.....	57
Gambar V.9 <i>Data flow diagram</i> dari <i>whaling attack</i> kombinasi serangan OSINT SpiderFoot, <i>social engineering</i> Dark-Phish, dan <i>email spoofing</i> Telnet	62
Gambar V.10 Diagram keterkaitan antara serangan OSINT, <i>social engineering</i> , <i>email spoofing</i> yang menghasilkan <i>whaling attack</i>	67
Gambar V.11 <i>Attack tree</i> dari <i>whaling attack</i> OSINT Knockpy, <i>social engineering</i> SEToolkit, dan <i>email spoofing</i> Telnet.....	68
Gambar V.12 <i>Attack tree</i> dari <i>whaling attack</i> OSINT Skymem, <i>social engineering</i> Dark-Phish, dan <i>email spoofing</i> Telnet.....	70
Gambar V.13 <i>Attack tree</i> dari <i>whaling attack</i> OSINT SpiderFoot, <i>social engineering</i> Dark-Phish, dan <i>email spoofing</i> Telnet.....	72
Gambar V.14 Hasil pengembangan <i>attack tree</i> dari <i>whaling attack</i>	74
Gambar V.15 Grafik perbandingan metrik <i>time</i> dari <i>whaling attack</i>	79
Gambar V.16 <i>Attack tree diagram</i> dari <i>whaling attack</i> beserta metrik <i>time</i>	81