

DAFTAR GAMBAR

Gambar III.1 Model Konseptual Penelitian	16
Gambar III.2 Sistematika Penelitian	18
Gambar IV.1 Perangkat <i>Platform</i> Eksperimen	25
Gambar IV.2 Alur Eksperimen Menggunakan OSINT <i>Tool</i> TheHarvester	27
Gambar IV.3 Alur Eksperimen Menggunakan OSINT <i>Tool</i> Metagoofil	28
Gambar IV.4 Alur Eksperimen Menggunakan OSINT <i>Tool</i> Recon-ng.....	30
Gambar IV.5 Alur Eksperimen Menggunakan OSINT <i>Tool</i> Snov.io.....	32
Gambar IV.6 Alur Eksperimen Menggunakan <i>Social Engineering Tool</i> SEToolkit	34
Gambar IV.7 Alur Eksperimen Menggunakan <i>Social Engineering Tool</i> Zphisher	36
Gambar IV.8 Alur Eksperimen <i>Email Spoofing</i> Menggunakan Telnet	38
Gambar IV.9 Implementasi OSINT <i>Tool</i> TheHarvester Proses <i>Input</i>	40
Gambar IV.10 Implementasi OSINT <i>Tool</i> TheHarvester <i>Output</i>	40
Gambar IV.11 Impementasi OSINT <i>Tool</i> Metagoofil Proses <i>Input</i> dan <i>Output</i>	41
Gambar IV.12 Implementasi OSINT <i>Tool</i> Recon-ng Proses <i>Input</i>	42
Gambar IV.13 Implementasi OSINT <i>Tool</i> Recon-ng <i>Output</i> dari <i>Modules</i> Hackertarget	42
Gambar IV.14 Implementasi OSINT <i>Tool</i> Recon-ng <i>Output</i> dari <i>Modules</i> Brute_host	43
Gambar IV.15 Implementasi OSINT <i>Tool</i> Snov.io Proses <i>Input</i>	43
Gambar IV.16 Implementasi OSINT <i>Tool</i> Snov.io <i>Output</i>	44
Gambar IV.17 Implementasi <i>Social Engineering Tool</i> SEToolkit Proses <i>Input</i> 1	45
Gambar IV.18 Implementasi <i>Social Engineering Tool</i> SEToolkit Proses <i>Input</i> 2	45
Gambar IV.19 Impementasi <i>Social Engineering Tool</i> SEToolkit <i>Output</i>	46
Gambar IV.20 Implementasi <i>Social Engineering Tool</i> Zphisher Proses <i>Input</i> ...	47
Gambar IV.21 Impementasi <i>Social Engineering Tool</i> Zphisher <i>Output</i> Tampilan <i>Cloned Website</i>	47
Gambar IV.22 Implementasi <i>Social Engineering Tool</i> <i>Output</i> Data Kredensial	48

Gambar IV.23 Implementasi Pengiriman <i>Email Spoofing</i> Menggunakan Telnet Proses <i>Input</i>	49
Gambar IV.24 Implementasi Pengiriman <i>Email Spoofing</i> Menggunakan Telnet <i>Output</i>	49
Gambar V.1 Hasil Perumusan Berdasarkan Serangan OSINT <i>Tool</i> TheHarvester	63
Gambar V.2 Hasil Perumusan Berdasarkan Serangan OSINT <i>Tool</i> Metagoofil	64
Gambar V.3 Hasil Perumusan Berdasarkan Serangan OSINT <i>Tool</i> Recon-ng ..	65
Gambar V.4 Hasil Perumusan Berdasarkan Serangan OSINT <i>Tool</i> Snov.io	66
Gambar V.5 Hasil Perumusan Berdasarkan Serangan <i>Social Engineering Tool</i> SEToolkit	67
Gambar V.6 Hasil Perumusan Berdasarkan Serangan <i>Social Engineering Tool</i> Zphisher.....	69
Gambar V.7 Hasil Perumusan Berdasarkan Serangan <i>Email Spoofing</i> Menggunakan Telnet.....	70
Gambar V.8 Konsep Penyerangan <i>Spear Phishing Attack</i>	71
Gambar V.9 Hasil Perumusan <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT TheHarvester, <i>Social Engineering</i> SEToolkit, dan <i>Email Spoofing</i>	76
Gambar V.10 Hasil Perumusan <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Metagoofil, <i>Social Engineering</i> Zphisher, dan <i>Email Spoofing</i>	79
Gambar V.11 Hasil Perumusan <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Recon-ng, <i>Social Engineering</i> SEToolkit, dan <i>Email Spoofing</i>	83
Gambar V.12 Hasil Perumusan <i>Spear Phishing Attack</i> Berdasarkan Serangan OSINT Snov.io, <i>Social Engineering</i> Zphisher, dan <i>Email Spoofing</i>	87
Gambar V.13 <i>Attack Tree</i> I <i>Spear Phishing Attack</i>	90
Gambar V.14 <i>Attack Tree</i> II <i>Spear Phishing Attack</i>	92
Gambar V.15 <i>Attack Tree</i> III <i>Spear Phishing Attack</i>	95
Gambar V.16 <i>Attack Tree</i> IV <i>Spear Phishing Attack</i>	98
Gambar V.17 Hasil <i>Attack Tree</i> Berdasarkan <i>Spear Phishing Attack</i>	100
Gambar V.18 Grafik Perbandingan Metrik Granularitas Data	106
Gambar V.19 Diagram <i>Attack Tree</i> dengan Metrik Granularitas Data.....	108