

DAFTAR GAMBAR

Gambar III- 1. Metode konseptual	13
Gambar III- 2. Sistematika penyelesaian masalah	15
Gambar IV- 1. Alur eksperimen OSINT <i>tools</i> berbasis CLI	26
Gambar IV- 2. Alur eksperimen OSINT <i>tools</i> berbasis <i>website</i>	27
Gambar IV- 3. Alur eksperimen OSINT <i>tools</i> berbasis <i>extension</i>	28
Gambar IV- 4. Implementasi eksperimen menggunakan <i>tool</i> whois	29
Gambar IV- 5. Implementasi eksperimen menggunakan <i>tool</i> nslookup	30
Gambar IV- 6. Implementasi eksperimen menggunakan <i>tool</i> Shodan.....	31
Gambar IV- 7. Implementasi eksperimen menggunakan <i>tool</i> curl.....	32
Gambar IV- 8. Implementasi eksperimen menggunakan <i>tool</i> Wappalyzer.....	34
Gambar IV- 9. Implementasi eksperimen menggunakan <i>tool</i> nmap.....	35
Gambar IV- 10. Implementasi eksperimen menggunakan <i>tool</i> sslscan	37
Gambar IV- 11. Lanjutan implementasi eksperimen menggunakan <i>tool</i> sslscan..	38
Gambar IV- 12. Implementasi eksperimen menggunakan <i>tool</i> REDbot.....	39
Gambar IV- 13. Implementasi eksperimen menggunakan <i>tool</i> sublist3r	40
Gambar IV- 14. Lanjutan implementasi eksperimen menggunakan <i>tool</i> sublist3r	40
Gambar IV- 15. Implementasi eksperimen menggunakan <i>tool</i> Traceroute.....	41
Gambar IV- 16. Implementasi eksperimen menggunakan <i>tool</i> dirb	42
Gambar V- 1. <i>Data flow diagram</i> skenario <i>credential stuffing</i>	64
Gambar V- 2. <i>Attack tree</i> skenario <i>credential stuffing</i>	65
Gambar V- 3. <i>Data flow diagram</i> skenario <i>bruteforce login</i>	67
Gambar V- 4. <i>Attack tree</i> skenario <i>bruteforce login</i>	68
Gambar V- 5. <i>Data flow diagram</i> skenario <i>man-in-the-middle</i>	69
Gambar V- 6. <i>Attack tree</i> skenario <i>man-in-the-middle</i>	70