

DAFTAR GAMBAR

Gambar III-1 Model konseptual penelitian	15
Gambar III-2 Sistematisa penyelesaian masalah	17
Gambar IV-1 Alur eksperimen menggunakan OSINT <i>Tools</i> berbasis CLI.....	27
Gambar IV-2 Alur eksperimen menggunakan OSINT <i>Tools</i> berbasis <i>web</i>	28
Gambar IV-3 Alur eksperimen menggunakan OSINT <i>Tools</i> berbasis ekstensi peramban	29
Gambar IV-4 Implementasi eksperimen menggunakan OSINT <i>Tool</i> whois.....	30
Gambar IV-5 Implementasi eksperimen menggunakan OSINT <i>Tool</i> nslookup....	31
Gambar IV-6 Implementasi eksperimen menggunakan OSINT <i>Tool</i> amass.....	32
Gambar IV-7 Implementasi eksperimen menggunakan OSINT <i>Tool</i> theHarvester	33
Gambar IV-8 Implementasi eksperimen menggunakan OSINT <i>Tool</i> curl	34
Gambar IV-9 Implementasi eksperimen menggunakan OSINT <i>Tool</i> nmap	35
Gambar IV-10 Implementasi eksperimen menggunakan OSINT <i>Tool</i> dmitry.....	36
Gambar IV-11 Implementasi eksperimen menggunakan OSINT <i>Tool</i> sslscan	37
Gambar IV-12 Cuplikan <i>output</i> menggunakan OSINT <i>Tool</i> sslscan dalam format .txt	38
Gambar IV-13 Implementasi eksperimen menggunakan OSINT <i>Tool</i> Shodan	39
Gambar IV-14 Implementasi eksperimen menggunakan OSINT <i>Tool</i> REDbot ...	40
Gambar IV-15 Implementasi eksperimen menggunakan OSINT <i>Tool</i> Wappalyzer	41
Gambar V-1 <i>Data Flow Diagram</i> skenario <i>Credential Sniffing</i>	69
Gambar V-2 <i>Attack Tree</i> skenario <i>Credential Sniffing</i>	70
Gambar V-3 <i>Data Flow Diagram</i> skenario <i>Remote Code Execution</i>	71
Gambar V-4 <i>Attack Tree</i> skenario <i>Remote Code Execution</i>	72
Gambar V-5 <i>Data Flow Diagram</i> skenario <i>Cloud Misconfiguration</i>	74
Gambar V-6 <i>Attack Tree</i> skenario <i>Cloud Misconfiguration</i>	75