

DAFTAR GAMBAR

Gambar III.1 Model Konseptual	13
Gambar III.2 Sistematika Penyelesaian Masalah.....	15
Gambar IV.1 Platform Eksperimen	23
Gambar IV.2 Skenario Pengujian Eksploitasi.....	25
Gambar IV.3 Skenario Pengujian Serangan Berdasarkan <i>Activity Diagram</i> dan <i>Data Flow Diagram</i>	26
Gambar IV.4 Skenario Eksploitasi Pengujian XML-RPC.....	28
Gambar IV.5 Perumusan Serangan Dengan <i>Activity Diagram</i> Berdasarkan Eksploitasi Kerentanan XML-RPC.....	31
Gambar IV.6 Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi Kerentanan XML-RPC.....	32
Gambar IV.7 Proses Enumerasi WordPress Menggunakan WPScan.....	33
Gambar IV.8 Hasil Eksploitasi Kerentanan XML-RPC	34
Gambar IV.9 Skenario Eksploitasi Pengujian DDoS.....	36
Gambar IV.10 Perumusan Serangan Dengan <i>Activity Diagram</i> Berdasarkan Eksploitasi DDoS	39
Gambar IV.11 Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi DDoS	40
Gambar IV.12 Proses serangan DDoS menggunakan Hping3.....	41
Gambar IV.13 Paket Pada Wireshark Saat Serangan DDoS Berlangsung	42
Gambar IV.14 Skenario Eksploitasi Pengujian <i>Packet Sniffing</i>	44
Gambar IV.15 Perumusan Serangan Dengan <i>Activity Diagram</i> Berdasarkan Eksploitasi <i>Packet Sniffing</i>	47
Gambar IV.16 Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi <i>Packet Sniffing</i>	48
Gambar IV.17 Proses Pemilihan <i>Host</i> Target Pada Ettercap.....	50
Gambar IV.18 Hasil Eksploitasi <i>Packet Sniffing</i>	50
Gambar IV.19 Skenario Eksploitasi Pengujian <i>Packet Data Manipulation</i>	52
Gambar IV.20 Perumusan Serangan Dengan <i>Activity Diagram</i> Berdasarkan Eksploitasi <i>Packet Data Manipulation</i>	55

Gambar IV.21 Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi <i>Packet Data Manipulation</i>	56
Gambar IV.22 Hasil <i>Scanning Host</i> Target Pada Bettercap	57
Gambar IV.23 Konfigurasi Pada Eksploitasi <i>Packet Data Manipulation</i>	58
Gambar IV.24 Skenario Eksploitasi Pengujian <i>Session Hijacking</i>	60
Gambar IV.25 Perumusan Serangan Dengan <i>Activity Diagram</i> Berdasarkan Eksploitasi <i>Session Hijacking</i>	64
Gambar IV.26 Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi <i>Session Hijacking</i>	65
Gambar IV.27 Proses Mendapatkan <i>Session Cookie</i> Pada <i>Host</i> Target	67
Gambar IV.28 Proses Pengubahan <i>Session Cookie</i> Pada Burp Suite	67