

DAFTAR TABEL

Tabel II.1 Penelitian Terdahulu.....	11
Tabel IV.1 Spesifikasi Perangkat Keras.....	18
Tabel IV.2 Spesifikasi Perangkat Lunak.....	20
Tabel IV.3 Daftar Alamat IP	24
Tabel IV.4 Hasil Perumusan Serangan Berdasarkan Eksploitasi XML-RPC.....	29
Tabel IV.5 Data Hasil Pengujian Eksploitasi XML-RPC.....	34
Tabel IV.6 Hasil Perumusan Serangan Berdasarkan Eksploitasi DDoS.....	37
Tabel IV.7 Data Hasil Pengujian Eksploitasi DDoS.....	42
Tabel IV.8 Hasil Perumusan Serangan Berdasarkan Eksploitasi <i>Packet Sniffing</i>	45
Tabel IV.9 Data Hasil Pengujian Eksploitasi <i>Packet Sniffing</i>	51
Tabel IV.10 Hasil Perumusan Serangan Berdasarkan Eksploitasi <i>Packet Data Manipulation</i>	54
Tabel IV.11 Data Hasil Pengujian Eksploitasi <i>Packet Data Manipulation</i>	58
Tabel IV.12 Hasil Perumusan Serangan Berdasarkan Eksploitasi <i>Session Hijacking</i>	62
Tabel IV.13 Data Hasil Pengujian Eksploitasi <i>Session Hijacking</i>	68
Tabel V.1 Analisis Ancaman Terhadap Keamanan Data.....	69
Tabel V.2 Mekanisme <i>Disclosure</i> pada Hasil Pengujian Eksploitasi	71
Tabel V.3 Mekanisme <i>Alteration</i> pada Hasil Pengujian Eksploitasi	72
Tabel V.4 Mekanisme <i>Denial</i> pada Hasil Pengujian Eksploitasi	72
Tabel V.5 Analisis Ancaman Berdasarkan OWASP <i>Top Ten</i>	73
Tabel V.6 Identifikasi CVE ID dari Eksploitasi Pengujian	75
Tabel V.7 Penentuan Skor CVE Menggunakan CVSS.....	76
Tabel V.8 Penentuan Tingkat Keparahan Kerentanan.....	79
Tabel V.9 Strategi Mekanisme Keamanan.....	80
Tabel V.10 Desain Kontrol Keamanan Berdasarkan Kerentanan Yang Dieksploitasi oleh Ancaman	84
Tabel V.11 Mekanisme Keamanan Pada Kategori <i>Cryptographic Failures</i>	87
Tabel V.12 Mekanisme Keamanan Pada Kategori <i>Identification and Authentication Failures</i>	88

Tabel V.13 Mekanisme Keamanan Pada Kategori <i>Software and Data Integrity Failures</i>	90
Tabel V.14 Mekanisme Keamanan Pada Kategori <i>Security Logging and Monitoring Failures</i>	91