

DAFTAR ISI

KATA PENGANTAR.....	vi
DAFTAR ISI	vii
BAB I	
MANAJEMEN KEAMANAN SISTEM	
INFORMASI	1
1.1 Kejahatan komputer dan internet.....	4
1.2 Klasifikasi kejahatan Komputer	9
1.3 Seluk beluk dan istilah <i>Hacker</i>	10
1.4 Peningkatan jumlah <i>hacker</i>	12
1.5 Macam pengelompokan <i>Hacker</i>	13
1.6 Beberapa alasan <i>hacker</i> beroperasi	15
1.7 Cara <i>hacker</i> beroperasi	16
1.8 Cracker	19
1.9 Phreaker.....	20
1.10 Defacer.....	20
1.11 Aspek aspek dalam keamanan sistem informasi.....	21
1.12 Pengenalan metode keamanan sistem informasi.....	24
1.13 Standarisasi dalam Keamanan Sistem Informasi.....	32

BAB II	KERAWANAN DALAM SISTEM.....	35
2.1	Operating sistem attack/Kerawanan pada Sistem Operasi	36
2.2	Application level attacks/Kerawanan pada Level Aplikasi.....	38
2.3	Program application modul/Kerawanan pada Modul Program	40
2.4	Standar configuration/Kerawanan Akibat Konfigurasi Standar	40
BAB III	6 DOMAIN UTAMA DUNIA KEAMANAN SISTEM INFORMASI	43
3.1	Human (Manusia).....	44
3.2	<i>Threat</i> (Ancaman)	48
3.3	<i>Attack</i> (Serangan).....	50
3.4	<i>Method</i> (Metode).....	60
3.5	<i>Tools</i> (Alat)	62
3.6	<i>Risk</i> /Risiko	63
BAB IV	MANAJEMEN RISIKO	65
4.1	Aset Identification (Identifikasi Aset)	66
4.2	Threat Identification (Identifikasi ancaman)	67
4.3	Vulnerability (Kerawanan/kelemahan)	67
4.4	Probability of threats (Kemungkinan ancaman)	68
4.5	Analisa dampak (Impact analysis)	69

4.6	Menentukan nilai Risiko (Risk Value Identification).....	70
BAB V	PENILAIAN KEBIJAKAN KEAMANAN SISTEM INFORMASI BERDASARKAN ISO27001	71
5.1	Cara mengembangkan sebuah kebijakan keamanan	72
5.2	Kebutuhan untuk Kebijakan Keamanan Jaringan.....	73
5.3	Risiko dari Keterhubungan Jaringan	74
5.4	Komponen dari suatu Kebijakan Keamanan Jaringan.....	75
5.5	Langkah untuk mengembangkan suatu Kebijakan Keamanan Jaringan.....	79
5.6	Klausul <i>ISO27001</i>	82
BAB VI	Pengenalan Tools dalam Teknik Keamanan Sistem	93
BAB VII	CYBERSIX	101
7.1	Cyber Space.....	101
7.2	Cyber Threat	103
7.3	Cyber Attack.....	107
7.4	Cyber Security	110
7.5	Cyber Crime	113
7.6	Cyber Law.....	116
BAB VIII	Digital Evidence dan Komputer Forensik.....	121
8.1	Bukti digital	121

8.2	Sejarah penggunaan bukti digital	122
8.3	Sumber-sumber Bukti Digital	125
8.4	Forensik.....	128
8.5	Melacak Sumber Program Perusak	140
8.6	Analisis Unknown Program	142
8.7	Standard Metodologi Komputer Forensik.....	144
8.8	Perlunya Perlindungan Bukti	148
8.9	Pemrosesan Barang Bukti	151
REFERENSI		157
LAMPIRAN		159
PROFIL PENULIS		217