

DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN	ii
HALAMAN PENGESAHAN TUGAS AKHIR.....	iii
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR SIMBOL.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Tujuan Tugas Akhir	3
1.4 Manfaat Tugas Akhir	4
1.5 Lingkup Tugas Akhir	4
1.6 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Sistem Transportasi Laut.....	6
2.1.1 Infrastruktur Kapal	6
2.1.2 Infrastruktur Pelabuhan	9
2.2 Keamanan Siber	10
2.2.1 Serangan Siber.....	11
2.2.2 <i>Cybersecurity Framework</i>	12
2.2.3 <i>The CIA Model</i>	13
2.2.4 <i>Risk Assessment</i>	14
2.2.5 Elemen Keamanan Siber	17

2.3	Komunikasi Satelit	17
2.3.1	<i>Band</i> Frekuensi Satelit.....	18
2.3.2	Cara Kerja Satelit	19
2.3.3	Satelit VSAT (<i>Very Small Aperture Terminal</i>)	20
2.4	Jaringan Komputer	22
2.4.1	Jenis Jaringan Komputer	24
2.4.2	Topologi Jaringan Komputer.....	26
2.4.3	<i>IP Address</i>	28
2.4.4	<i>IP Public</i> dan <i>IP Private</i>	28
2.4.5	Kelas <i>IP Address</i>	29
2.4.6	<i>Subnet Mask</i>	29
2.4.7	<i>Classless Inter-Domain Routing (CIDR)</i>	29
2.4.8	Perangkat Keras Jaringan	30
2.4.9	Perangkat Lunak Jaringan	32
2.5	Sistem Informasi	33
2.6	Internet	33
2.7	Website.....	34
2.8	<i>Email</i>	34
2.9	<i>Mail Server</i>	35
2.10	VoIP	35
2.11	Remote Login.....	36
2.12	UML (<i>Unified Modeling Language</i>).....	36
2.13	Studi Literatur	37
BAB III	METODE PENELITIAN.....	42
3.1	Tempat Penelitian.....	42
3.2	Profil Perusahaan	42
3.2.1	Visi dan Misi	43
3.3	Metodologi Penelitian	44
3.4	Rencana Penelitian	44
3.5	Objek Penelitian	45
3.6	Topik Penelitian	45
3.7	Metode Pengumpulan Data	45

3.8	Tujuan Penelitian	47
3.9	Metode Penerapan Keamanan	47
3.9.1	<i>Framework</i> NIST.....	48
3.9.2	<i>The CIA Model</i>	49
3.9.3	<i>Risk Assessment</i>	49
3.10	Alat Penelitian	53
3.11	Skema Penelitian	54
3.11.1	Struktur Organisasi Kapal	54
3.11.2	Analisa <i>Cybercrime</i> Kapal	54
3.11.3	Analisa Jaringan Kapal.....	56
3.11.4	Simulasi Jaringan Kapal.....	58
3.11.5	Analisa Komputer Kapal	64
3.11.6	Analisa Aplikasi Komputer Kapal.....	64
3.12	Analisa Perangkat Komunikasi Kapal	65
3.13	Teknis Pengujian Keamanan.....	66
3.14	Analisa Hasil	66
3.15	Penulisan Laporan.....	66
BAB IV	HASIL DAN PEMBAHASAN.....	67
4.1	Data Hasil Penelitian.....	67
4.1.1	Analisa Masalah	67
4.1.2	Analisa Metode Keamanan.....	67
4.1.3	Analisa Kebutuhan Sistem (Fungsional dan Non-Fungsional)	70
4.1.4	Analisa Tahapan Keamanan Siber.....	71
4.2	Analisa Keamanan Siber	71
4.2.1	Identifikasi Kerentanan Siber	74
4.2.2	Infrastruktur Jaringan Kapal.....	77
4.2.3	Infrastruktur Komunikasi VSAT.....	79
4.2.4	Infrastruktur Komunikasi <i>Email</i>	80
4.3	Implementasi Keamanan Siber	81
4.3.1	Karakteristik dan Jenis <i>Firewall</i>	81
4.3.2	Pemasangan Perangkat <i>Firewall</i> dan ICM.....	82
4.3.3	Konfigurasi <i>IP Address</i> Pada <i>Firewall</i> Dan ICM.....	83

4.3.4	Konfigurasi <i>Port, Outbound, Inbound</i> Pada <i>Firewall</i>	84
4.4	Pengujian Keamanan Siber	86
4.4.1	<i>Mapping Network</i>	87
4.4.2	Akses VSAT	88
4.4.3	Akses Internet	89
4.4.4	Akses <i>Email</i>	89
4.4.5	Akses Jaringan Operasional Kerja	90
4.4.6	Akses Jaringan Operasional Kapal	91
4.5	<i>Monitoring</i> Keamanan Siber	92
4.5.1	<i>Monitoring Traffic</i> Komunikasi VSAT	92
4.5.2	<i>Monitoring Traffic</i> Komunikasi <i>Email</i>	94
4.6	<i>Recovery</i> Serangan Siber	95
4.7	Klasifikasi Serangan Siber	96
4.8	<i>Internal Risk Assessment</i>	99
4.8.1	Pengukuran <i>Risk Assessment</i>	99
4.8.2	Hasil <i>Risk Assessment</i>	99
BAB V	KESIMPULAN DAN SARAN	101
5.1	Kesimpulan	101
5.2	Saran	101
	DAFTAR PUSTAKA	103
	LAMPIRAN 1 DAFTAR RIWAYAT HIDUP	106
	LAMPIRAN 2 SURAT PERMOHONAN PENELITIAN	107
	LAMPIRAN 3 SURAT PENERIMAAN PENELITIAN	108
	LAMPIRAN 4 PERATURAN KEAMANAN SIBER	109
	LAMPIRAN 5 SURAT TUGAS KUNJUNGAN KAPAL	117
	LAMPIRAN 6 KEBIJAKAN KEAMANAN SIBER IBT	118
	LAMPIRAN 7 RISK ASSESSMENT REPORT	123

DAFTAR TABEL

Tabel 2.1 Komponen Infrastruktur Kapal	8
Tabel 2.2 <i>Band</i> Frekuensi	18
Tabel 2.3 Daftar Studi <i>Literatur</i>	37
Tabel 3.1 Kapal Milik IBT Group.....	43
Tabel 3.2 Pertanyaan Wawancara	45
Tabel 3.3 Level Tingkatan Sumber Ancaman.....	50
Tabel 3.4 Level Dampak Sumber Ancaman	51
Tabel 3.5 Level Risiko <i>Assessment</i>	52
Tabel 3.6 Tabel Pengalamatan IP <i>Address</i>	59
Tabel 3.7 Perangkat Komputer Kapal.....	64
Tabel 3.8 Perangkat Komunikasi Kapal.....	65
Tabel 4.1 Empat Fase Kunci <i>Respon Insiden Framework</i> NIST	67
Tabel 4.2 Analisis CIA Model	69
Tabel 4.3 <i>Risk Assessment Result</i>	70
Tabel 4.4 Kebutuhan <i>Fungsional</i>	70
Tabel 4.5 <i>Use Case Description Initial Assessment</i>	72
Tabel 4.6 <i>Use Case Description In-depth Assessment / 1st Pen Testing</i>	73
Tabel 4.7 <i>Use Case Description In-depth Assessment</i>	73
Tabel 4.8 <i>Use Case Description Issuance of Verification Statement</i>	73
Tabel 4.9 <i>Use Case Description Attack Techniques</i>	74
Tabel 4.10 <i>Use Case Description Security Barriers</i>	75
Tabel 4.11 <i>Use Case Description Computer Systems</i>	75
Tabel 4.12 <i>Use Case Description Usb Flashdisk Viruses and Malware</i>	76
Tabel 4.13 <i>Use Case Description Email Phishing</i>	77
Tabel 4.14 Tabel IP <i>Address</i>	83
Tabel 4.15 Akses <i>Service Port</i>	85
Tabel 4.16 Akses IP <i>Address</i>	85
Tabel 4.17 Klasifikasi Serangan Siber.....	97

DAFTAR GAMBAR


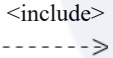
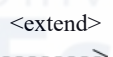

Gambar 2.1 <i>Vessel dan Port</i> Infrastruktur MTS	6
Gambar 2.2 Interaksi Elemen Arsitektur Kapal	6
Gambar 2.3 Infrastruktur Kapal	7
Gambar 2.4 Infrastruktur Pelabuhan	10
Gambar 2.5 Ruang Siber	10
Gambar 2.6 Serangan Siber Bersifat Teknis	11
Gambar 2.7 NIST <i>Cybersecurity Framework</i>	12
Gambar 2.8 <i>The CIA Model</i>	14
Gambar 2.9 <i>Risk Assessment Steps</i>	15
Gambar 2.10 Cara Kerja Komunikasi Satelit	19
Gambar 2.11 Arsitektur Jaringan VSAT	20
Gambar 2.12 <i>Hub Station</i>	21
Gambar 2.13 <i>Antenna Mini VSAT</i>	22
Gambar 2.14 Komponen <i>Outdoor dan Indoor Unit</i>	22
Gambar 2.15 <i>Peer to Peer Network</i>	23
Gambar 2.16 <i>Client Server Network</i>	24
Gambar 2.17 Jaringan LAN	24
Gambar 2.18 Jaringan MAN	25
Gambar 2.19 Jaringan WAN	25
Gambar 2.20 Jaringan WLAN	26
Gambar 2.21 Diagram Topologi <i>Bus</i>	26
Gambar 2.22 Diagram Topologi <i>Ring</i>	27
Gambar 2.23 Diagram Topologi <i>Star</i>	27
Gambar 2.24 Diagram Topologi <i>Mesh</i>	28
Gambar 2.25 IPv4 32 <i>Binary Bits</i>	28
Gambar 2.26 Kelas IP <i>Address</i>	29
Gambar 2.27 Alokasi IP <i>Private</i> Dengan CIDR	30
Gambar 2.28 <i>Hub</i>	30
Gambar 2.29 <i>Network Interface Card (NIC)</i>	31
Gambar 2.30 <i>Router</i>	31
Gambar 2.31 <i>Switch</i>	31
Gambar 2.32 <i>Access Point (AP)</i>	32
Gambar 2.33 <i>Voice over Internet Protocol (VoIP)</i>	35
Gambar 3.1 Langkah-Langkah Penelitian	44
Gambar 3.2 <i>Framework NIST</i>	48
Gambar 3.3 <i>CIA Model Triad</i>	49
Gambar 3.4 <i>Risk Assessment Matrix (RAM)</i>	50
Gambar 3.5 <i>Residual Risk Assessment</i>	52
Gambar 3.6 <i>Initial Risk Score Assessment</i>	52



Gambar 3.7 <i>Antenna VSAT dan ICM KVH</i>	53
Gambar 3.8 <i>Netgear VPN Firewall</i>	53
Gambar 3.9 <i>Cybercrime Pada Kapal</i>	55
Gambar 3.10 <i>OSI Model dan Cyberattack</i>	56
Gambar 3.11 <i>Diagram Komunikasi VSAT</i>	57
Gambar 3.12 <i>Topologi Business Administration Network</i>	57
Gambar 3.13 <i>Topologi Operational Techonolgy Network</i>	58
Gambar 3.14 <i>Diagram Firewall 2 Layer</i>	58
Gambar 3.15 <i>Topologi Jaringan Kapal</i>	59
Gambar 3.16 <i>Hasil Ping Komputer Server</i>	60
Gambar 3.17 <i>Hasil Ping Laptop Email</i>	61
Gambar 3.18 <i>Hasil Ping Komputer Engine</i>	61
Gambar 3.19 <i>Hasil Ping Komputer Datalogger</i>	62
Gambar 3.20 <i>Hasil Ping Komputer OT Monitoring</i>	62
Gambar 3.21 <i>Hasil Simulasi Packet Antar jaringan</i>	63
Gambar 3.22 <i>Hasil Simulasi Packet dari OT Monitoring</i>	63
Gambar 4.1 <i>Use Case Diagram Analisa Keamanan Siber</i>	72
Gambar 4.2 <i>Use Case Diagram Serangan Siber</i>	74
Gambar 4.3 <i>Use Case Serangan Siber Insider</i>	76
Gambar 4.4 <i>Topologi Jaringan Pada Kapal Lama</i>	78
Gambar 4.5 <i>Topologi Jaringan Pada Kapal Baru</i>	79
Gambar 4.6 <i>Datalogger Engine Cargo Controller OT Network</i>	79
Gambar 4.7 <i>Network Diagram KVH VSAT</i>	80
Gambar 4.8 <i>Network Diagram GTMailPlus</i>	80
Gambar 4.9 <i>Flow Map Implementasi Keamanan Siber</i>	81
Gambar 4.10 <i>Topologi Jaringan Firewall</i>	82
Gambar 4.11 <i>Business Network Firewall</i>	82
Gambar 4.12 <i>OT Network Firewall</i>	83
Gambar 4.13 <i>Integrated CommBox Modem (ICM) VSAT</i>	83
Gambar 4.14 <i>Konfigurasi IP Address Firewall</i>	84
Gambar 4.15 <i>Konfigurasi IP Address VSAT ICM</i>	84
Gambar 4.16 <i>Service Port Firewall</i>	86
Gambar 4.17 <i>Outbound dan Inbound Firewall</i>	86
Gambar 4.18 <i>Mapping Network Operasional Kerja</i>	87
Gambar 4.19 <i>Mapping Network Operasional Kapal</i>	87
Gambar 4.20 <i>Koneksi LAN ICM KVH</i>	88
Gambar 4.21 <i>Portal KVH ICM</i>	88
Gambar 4.22 <i>Hasil Ping ke ICM VSAT</i>	89
Gambar 4.23 <i>Hasil Ping ke Internet</i>	89
Gambar 4.24 <i>Hasil Pengiriman dan Penerimaan Email</i>	90
Gambar 4.25 <i>Hasil Ping Operasional Kerja</i>	90
Gambar 4.26 <i>Hasil Ping Operasional Kapal</i>	91

Gambar 4.27 <i>Datalogger</i> Operasional Kapal	91
Gambar 4.28 <i>Flow Map Monitoring</i> Keamanan Siber.....	92
Gambar 4.29 Posisi Kapal dan Status VSAT.....	93
Gambar 4.30 <i>Traffic Monitoring</i> VSAT	93
Gambar 4.31 <i>Rules Email</i>	94
Gambar 4.32 Informasi <i>Email</i> Keluar.....	94
Gambar 4.33 Informasi <i>Email</i> Terima	95
Gambar 4.34 Informasi <i>Email</i> Ditolak.....	95
Gambar 4.35 <i>Flow Map Recovery</i> Serangan Siber	96
Gambar 4.36 <i>Initial Risk Acceptance System</i>	99
Gambar 4.37 <i>Final Score Risk Assessment</i>	99
Gambar 4.38 Hasil <i>Risk Assessment</i>	100






DAFTAR SIMBOL

Simbol *Use Case* Diagram (Yasin, 2012)



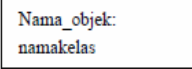
No	Simbol	Nama	Keterangan
1		<i>Actor</i>	Orang, proses atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi itu sendiri.
2		<i>Dependency</i>	Hubungan di mana perubahan yang terjadi pada suatu elemen mandiri (<i>independent</i>) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (<i>independent</i>).
3		<i>Generalization</i>	Hubungan generalisasi dan spesialisasi (umum-khusus) antar dua buah <i>use case</i> di mana fungsi yang satu adalah fungsi yang lebih umum dari yang lainnya.
4		<i>Include</i>	Relasi <i>use case</i> tambahan ke sebuah <i>use case</i> , di mana <i>use case</i> yang ditambahkan dapat berdiri sendiri.
5		<i>Extend</i>	Relasi <i>use case</i> tambahan ke sebuah <i>use case</i> , di mana <i>use case</i> yang ditambahkan memerlukan <i>use case</i> ini untuk menjalankan fungsinya atau sebagai syarat dijalankan <i>use case</i> ini.
6		<i>Association</i>	Komunikasi antar aktor dan <i>use case</i> yang berpartisipasi pada <i>use case</i> atau <i>use case</i> memiliki interaksi dengan aktor.
7		<i>System</i>	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		<i>Use Case</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu <i>actor</i> .



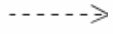
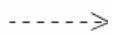
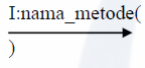
9		<i>Collaboration</i>	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan perilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

Simbol *Activity Diagram* (Yasin, 2012)




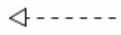
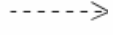
No	Simbol	Nama	Keterangan
1		Aktivitas	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		<i>Decision</i> /percabangan	Asosiasi percabangan di mana jika ada pilihan aktivitas lebih dari satu.
3		<i>Initial Node</i>	Bagaimana objek di bentuk atau diawali.
4		<i>Activity Final Node</i>	Bagaimana objek di bentuk dan dihancurkan.
5		<i>Fork Node</i>	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran.


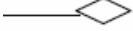
Simbol *Sequence Diagram* (Yasin, 2012)

No	Simbol	Nama	Keterangan
1		<i>Actor</i>	Orang, proses atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi itu sendiri..
2		<i>LifeLine</i>	Objek <i>entity</i> , antarmuka yang saling berinteraksi.
3		<i>Objek</i>	Menyatakan objek yang berinteraksi oleh pesan.

4		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
5		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi.
6	T-keluaran 	<i>Pesan tipe return</i>	Menyatakan bahwa suatu objek yang telah menjalankan suatu operasi atau metode menghasilkan suatu kembalian ke objek tertentu, arah panah mengarah pada objek yang menerima kembalian.
7	T-masukkan 	<i>Pesan tipe send</i>	Menyatakan bahwa suatu objek mengirim data/masukan/informasi ke objek lainnya, arah panah mengarah pada objek yang di kirim.
8		<i>Pesan tipe call</i>	Menyatakan suatu objek memanggil operasi/metode yang ada pada objek lain atau dirinya sendiri.

Simbol *Class Diagram* (Yasin, 2012)

No	Simbol	Nama	Keterangan
1		<i>Association</i>	Hubungan antarkelas dengan makna umum, asosiasi biasanya juga disertai dengan <i>multiplicity</i> .
2		<i>Nary Association</i>	Upaya untuk menghindari asosiasi dengan lebih dari 2 objek.
3		<i>Class</i>	Himpunan dari objek-objek yang berbagi atribut serta operasi yang sama.
4		<i>Realization</i>	Operasi yang benar-benar dilakukan oleh suatu objek.
5		<i>Dependency</i>	Hubungan di mana perubahan yang terjadi pada suatu elemen mandiri (independent) akan memengaruhi elemen yang bergantung padanya elemen yang tidak mandiri.

6		<i>Generalization</i>	Hubungan generalisasi dan spesialisasi (umum-khusus) antar dua buah <i>use case</i> di mana fungsi yang satu adalah fungsi yang lebih umum dari yang lainnya.
7		<i>Agregasi/ Aggregation</i>	Hubungan antar kelas dengan makna semua-bagian (<i>whole part</i>).