BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem transportasi laut bergantung pada komputasi dan komunikasi, memanfaatkan teknologi dalam bentuk digitalisasi, konektivitas, dan integrasi. Kemajuan teknologi internet berdampak pada pola komunikasi, dan kapal sudah menggunakan teknologi satelit untuk mempercepat jalur komunikasi dengan pemilik kapal dan otoritas terkait, mengirimkan pesan dan informasi baik ke kapal maupun pihak di darat. Dengan terkoneksinya kapal pada jaringan internet, maka tingkat risiko kerentanan akibat kejahatan siber semakin meningkat.

Pada Februari 2019, sebuah kapal *Deep Draft* dalam pelayaran internasional menuju pelabuhan *New York* dan *New Jersey* melaporkan bahwa mereka mengalami insiden serangan siber yang signifikan dan berdampak pada jaringan kapal. Sebuah tim ahli siber yang dipimpin oleh US *Coast Guard* menanggapi dan melakukan analisis terhadap jaringan kapal dan sistem kontrol. Hasil temuan menyimpulkan bahwa *malware* secara signifikan menurunkan fungsionalitas pada sistem komputer *onboard*, sedangkan sistem kontrol kapal tidak terpengaruh. Dari kejadian tersebut ditemukan kerentanan bahwa kapal beroperasi tanpa langkah-langkah keamanan siber yang efektif dapat mengekspos sistem kontrol kapal yang kritis terhadap kerentanan signifikan (US Coast Guard, 2019).

Perkembangan sektor industri maritim yang semakin bergerak menuju tingkat layanan digital pada pelabuhan dan kapal *autonomous*, membutuhkan protokol keamanan siber untuk peningkatan langkah-langkah perlindungan. Pelabuhan atau kapal berisiko terkena serangan siber jika sistem informasi utama tidak dilindungi secara memadai (Ben Farah et al., 2022). Bagaimana langkah-langkah keamanan siber yang harus dilakukan kapal dalam mengeksplorasi fasilitas navigasi kapal yang saling berhubungan dan dapat menjadi ancaman siber, bagaimana *hacker* membuat sinyal GPS (Lee et al., 2017).

Pada jaringan VSAT yang tidak memiliki enkripsi lapisan dasar dan VSAT menjadi ancaman baru terhadap kapal yang dapat di eksploitasi oleh berbagai

serangan siber (Pavur et al., 2020). Anomali dalam pesan NMEA dapat disebabkan oleh *cyberattack*, data NMEA membawa informasi yang sangat penting untuk beberapa fungsi navigasi, seperti penghindaran tabrakan (Amro et al., 2022). Sehingga diperlukan metode penilaian risiko yang didasarkan pada identifikasi kelompok serangan yang berpotensial, kerentanan komponen sistem, skenario serangan dan peringkat berdasarkan pedoman khusus (Bolbot et al., 2020). Penggunaan *Framework* NIST dapat mendukung organisasi dalam pendekatan penilaian risiko, dengan membantu memahami pendekatan yang efektif dalam mengelola potensi risiko siber. *Framework* CIA menjadi bagian dari penilaian kerentanan OT *systems onboard* yang berfokus pada ketersediaan dan integritas data. RAM (*Risk Assessment Matrix*) merupakan penilaian risiko yang mengukur dampak peristiwa keamanan siber berdasarkan kategori tertentu (BIMCO, 2021).

Menurut Surat Edaran Direktur Jenderal Perhubungan Darat Nomor SE.35 Tahun 2020, sistem informasi transportasi laut yang memiliki kerentanan ancaman jaringan maya (*cyberattack*) meliputi hal-hal sebagai berikut: sistem anjungan atau ruang navigasi, sistem manajemen penanganan muatan, manajemen tenaga penggerak dan permesinan serta sistem kontrol daya, sistem kontrol akses, sistem pelayanan dan penanganan penumpang, jaringan publik untuk penumpang, sistem administrasi dan kesejahteraan karyawan, dan sistem komunikasi.

Permasalahan yang dihadapi PT Indobaruna Bulk Transport (IBT) diperlukan sistem tahapan proses dan penilaian risiko keamanan siber (*cyber risk assessment*) pada kapal, bagian dari *safety committee*. Sehingga kerentanan sistem transportasi laut pada infrastruktur kapal terhadap serangan siber dapat diukur secara akurat dan efektif. Dampak penilaian risiko keamanan siber pada sistem transportasi laut yang belum terukur, mengakibatkan pemilik kapal (*shipowner*) tidak dapat memberikan kepastian proteksi keamanan siber terhadap penyewa kapal (*charter*).

Berdasarkan permasalahan di atas, maka perlu dilakukan analisis kondisi infrastruktur kapal meliputi: jaringan kapal, pengujian jaringan, keamanan jaringan dan perangkat kapal, serta membuat rekomendasi penilaian keamanan, sebagai langkah dalam penerapan keamanan siber sistem transportasi laut pada infrastruktur

kapal. Dalam penelitian ini penulis diberikan kesempatan oleh IBT sebagai tempat studi kasus dalam menganalisa keamanan siber pada kapal miliknya. IBT merupakan perusahaan pelayaran yang bergerak di kapal cargo khusus semen curah, memiliki jumlah armada sebanyak 15 (lima belas) kapal dengan area pelayaran meliputi domestik maupun internasional.

Oleh karena itu topik penelitian yang akan dilakukan adalah "Penerapan Keamanan Siber Pada Sistem Transportasi Laut (Studi Kasus: PT Indobaruna Bulk Transport)". Adanya penerapan keamanan siber pada infrastruktur kapal diharapkan dapat meningkatkan kepercayaan bagi rekanan dan keamanan khususnya bagi seluruh pihak.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dikemukan di atas, masalah tersebut dapat diidentifikasi sebagai berikut:

1. Bagaimana struktur sistem transportasi laut?
2. Bagaimana penerapan keamanan siber sistem transportasi laut pada infrastruktur kapal?
3. Bagaimana penilaian keamanan siber sistem transportasi laut pada infrastruktur kapal agar dapat terukur secara akurat dan efektif?

1.3 Tujuan Tugas Akhir

Berdasarkan identifikasi masalah yang telah dikemukan di atas, tujuan dari Tugas Akhir ini adalah sebagai berikut:

1. Mengetahui jenis-jenis ancaman keamanan siber sistem transportasi laut pada infrastruktur kapal.
2. Membuat langkah penerapan dan pengujian keamanan siber sistem transportasi laut pada infrastruktur kapal.
3. Membuat penilaian *cyber risk assessment* sehingga proteksi keamanan siber sistem transportasi laut pada infrastruktur kapal dapat terukur secara akurat dan efektif.

1.4 Manfaat Tugas Akhir

Berdasarkan latar belakang yang telah dikemukan di atas, manfaat dari Tugas Akhir ini adalah sebagai berikut:

1. Memberikan informasi mengenai topologi jaringan dan list perangkat pada infrastruktur kapal yang berdampak terhadap *cyber risks*.
2. Memberikan wawasan dan pengetahuan terhadap perangkat keamanan *cyber* yang digunakan pada infrastruktur kapal.
3. Memberikan solusi untuk internal *cyber risk assessment* sehingga keamanan siber pada infrastruktur kapal dapat terukur dengan baik.

1.5 Lingkup Tugas Akhir

Ruang lingkup pembahasan Tugas Akhir diutamakan pada masalah-masalah, sebagai berikut:

1. Analisa sistem transportasi laut pada infrastruktur kapal.
2. Penerapan keamanan siber sistem transportasi laut pada infrastruktur kapal.
3. Membuat *cyber risk management* pada infrastruktur kapal.

1.6 Sistematika Penulisan

Struktur penulisan makalah Tugas Akhir ini diuraikan dalam lima bab, dan isi dari bab-bab tersebut dijelaskan sebagai berikut:

BAB 1: PENDAHULUAN

Pada bab ini dibahas mengenai latar belakang masalah, identifikasi masalah, tujuan dan manfaat penelitian, lingkup tugas akhir serta sistematika penulisan laporan penelitian.

BAB 2: TINJAUAN PUSTAKA

Pada bab ini dijelaskan teori-teori penunjang yang digunakan sebagai dasar dalam komponen penelitian Penerapan Keamanan Siber Sistem Transportasi Laut pada infrastruktur kapal.

BAB 3: METODE PENELITIAN

Pada bab ini membahas tentang cara kerja metode yang digunakan dalam proses pembuatan seperti rencana penelitian, objek penelitian, kerangka berpikir dan teknik pengumpulan data.

BAB 4: HASIL DAN PEMBAHASAN

Pada bab ini berisi hasil penerapan keamanan siber sistem transportasi laut pada infrastruktur kapal di PT Indobaruna Bulk Transport.

BAB 5: KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari penelitian yang dibuat serta saran terkait dengan pengembangan sistem kedepannya.