BAB I PENDAHULUAN

I.1 Latar Belakang

Di era digital, *Open-Source Intelligence* (OSINT) berperan penting dalam mendukung identifikasi risiko melalui informasi terbuka. Menurut Khera (dalam Nagendran, 2024), OSINT melibatkan pengumpulan informasi dari sumber-sumber terbuka dan dapat diakses publik untuk mendapatkan wawasan terhadap target potensial. Metode ini dapat dimanfaatkan oleh aktor ancaman untuk mendeteksi kerentanan dan merancang ancaman siber secara sistematis. Menurut Abdul Razzaq (2021), ancaman siber adalah kondisi atau kemampuan yang berpotensi menimbulkan gangguan, kerusakan, dan kerugian, terutama terkait kerahasiaan, ketersediaan, dan integritas informasi. Ancaman ini bersifat potensial dan belum tentu terjadi, tetapi dapat berdampak pada sistem elektronik melalui perangkat digital (Abdul Razzaq Matthew Aditya et al., 2022).

Salah satu sektor yang sangat rentan terhadap ancaman siber adalah sektor perbankan. Menurut laporan *IBM X-Force Threat Intelligence Index* 2024, sektor keuangan dan asuransi menjadi industri yang paling banyak diserang secara global selama tiga tahun berturut-turut dengan 18,9% insiden pada 2023 menargetkan sektor ini (IBM, 2025). Di Indonesia sendiri, data dari Lanskap Keamanan Siber Indonesia 2024 dari BSSN mencatat sektor keuangan sebagai sektor prioritas dengan 9 dugaan insiden dan proporsi 3,58% dari total 56.128.160 data *exposure* sepanjang 2024 (BSSN, 2024). Meskipun persentasenya lebih kecil dibanding sektor pemerintahan, temuan ini tetap menunjukkan sektor keuangan memiliki tingkat risiko tinggi karena karakteristik datanya yang sensitif dan bernilai.

Sebelum memfokuskan penelitian pada sektor perbankan, dilakukan eksplorasi awal terhadap *platform* promotor konser bagian dari *entertainment event management* yang juga memiliki eksposur digital tinggi. Namun, hasil eksplorasi menunjukkan bahwa aset digital yang dimiliki relatif terbatas dan tidak cukup merepresentasikan nilai strategis yang dibutuhkan untuk analisis risiko berbasis OSINT. Berdasarkan pertimbangan tersebut, fokus penelitian dialihkan ke Institusi

Keuangan Syariah yang dalam hal ini akan disebut sebagai IKS, merupakan entitas keuangan dengan sistem digital yang aktif dan aset informasi yang bersifat kritikal. Pemilihan IKS juga diperkuat oleh ketersediaan data sekunder dari Publikasi Nasional, yang memungkinkan identifikasi dan estimasi nilai aset digital secara lebih terukur. Pendekatan OSINT diterapkan untuk menghimpun informasi terbuka mengenai potensi kerentanan dan eksposur digital *domain* IKS, memungkinkan analisis risiko tanpa memerlukan akses langsung ke sistem internal.

I.2 Perumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan di atas, maka rumusan permasalahan untuk penelitian ini adalah:

1. Bagaimana pola *information gathering* melalui OSINT dapat digunakan untuk mengidentifikasi potensi kerentanan pada layanan IT IKS?
2. Bagaimana potensi ancaman siber dapat disusun berdasarkan pendekatan hipotetis dari OSINT untuk menentukan tingkat risiko layanan IT pada IKS?
3. Bagaimana profil risiko IT setiap bank pada kategori aset organisasi IKS dapat digambarkan berdasarkan analisis risiko yang telah dilakukan?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menyusun pola pendekatan OSINT untuk mengidentifikasi potensi kerentanan pada layanan IT IKS melalui aktivitas pengumpulan informasi terhadap *domain* yang terbuka secara publik.
2. Mengimplementasikan penyusunan potensi ancaman siber berdasarkan pendekatan hipotetis dari OSINT untuk mengestimasi risiko layanan IT IKS.
3. Menggambarkan profil risiko IT setiap bank pada kategori aset organisasi IKS berdasarkan hasil estimasi risiko yang telah dilakukan.

I.4 Batasan Penelitian

Adapun batasan penelitian ini adalah:

1. Penelitian ini membatasi fokus pada aktivitas *profiling* risiko melalui tahap *information gathering* menggunakan OSINT, tanpa melakukan eksploitasi langsung terhadap sistem target. Selain itu, penentuan nilai kerentanan dan ancaman potensial mengacu pada jumlah temuan yang teridentifikasi, tanpa adanya penerapan skema pembobotan berdasarkan tingkat keparahan.
2. Penelitian ini tidak membahas aspek mitigasi, penanganan ancaman, perancangan terkait kebijakan, serta tata kelola melainkan berfokus pada identifikasi dan analisis potensi risiko dari sisi eksternal.
3. Objek penelitian dibatasi pada IKS yang memiliki data nilai aset dalam satuan rupiah dan berasal dari publikasi nasional (sebagai sumber data sekunder), tanpa melakukan penilaian langsung terhadap kondisi internal masing-masing bank.

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Secara teoritis
   a. Memperluas wawasan dan pemahaman mengenai pendekatan OSINT dalam analisis risiko keamanan siber, khususnya pada sektor perbankan.
   b. Memperkaya studi mengenai *risk profiling* berbasis OSINT melalui pengenalan kerangka kuantitatif yang menggabungkan unsur kerentanan (V), ancaman (T), dan aset (A) sebagai dasar perhitungan risiko terhadap layanan IT.
2. Secara praktis
   a. Memberikan gambaran mengenai fungsi OSINT dalam proses identifikasi kerentanan dan ancaman terhadap *domain* layanan IT, sehingga dapat digunakan sebagai pendekatan awal dalam asesmen keamanan eksternal.
   b. Menyediakan ilustrasi visual melalui *Data Flow Diagram* (DFD) dan *Attack Tree* untuk memetakan kemungkinan alur serangan berdasarkan temuan

OSINT, yang dapat dimanfaatkan sebagai bahan evaluasi oleh institusi keuangan atau praktisi keamanan informasi.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi rumusan masalah mengenai potensi kerentanan dan ancaman siber pada layanan IT IKS yang ditemukan melalui OSINT, serta bagaimana cara menghitung risiko terhadap layanan IT bank berdasarkan hasil identifikasi ancaman, kerentanan, dan aset dari data publik. Tujuan penelitian ini adalah menyusun pola pendekatan OSINT untuk mengidentifikasi potensi kerentanan pada layanan IT IKS melalui aktivitas pengumpulan informasi terhadap *domain* yang terbuka secara publik, mengimplementasikan penyusunan potensi ancaman siber berdasarkan pendekatan hipotetis dari OSINT untuk mengestimasi risiko layanan IT IKS, serta menggambarkan profil risiko IT setiap bank pada kategori aset organisasi IKS berdasarkan hasil estimasi risiko yang telah dilakukan. Penelitian ini juga menganalisis posisi OSINT dalam tahapan serangan melalui *Data Flow Diagram* dan model *Attack Tree*. Batasan masalah dalam penelitian ini adalah hanya mencakup aktivitas *profiling* estimasi risiko pada tahap *information gathering* menggunakan OSINT tanpa eksploitasi langsung, tidak membahas aspek mitigasi atau penanganan ancaman, serta hanya meneliti IKS yang memiliki data aset dalam rupiah dan tercantum dalam publikasi nasional. Manfaat penelitian ini secara teoretis adalah memperluas wawasan tentang pendekatan OSINT dalam analisis risiko keamanan siber, serta memperkaya studi *risk profiling* berbasis OSINT melalui kerangka kuantitatif. Dari sisi praktis, penelitian ini memberikan gambaran nyata mengenai fungsi OSINT dalam identifikasi kerentanan dan ancaman terhadap *domain* layanan IT, serta menyediakan ilustrasi

visual berupa DFD dan *Attack Tree* yang dapat dimanfaatkan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi literatur atau teori yang relevan dengan permasalahan yang diteliti, meliputi topik-topik seperti data publik, *risk assessment*, *Open-Source Intelligence* (OSINT), *information gathering*, *cyber profiling*, *threat modeling*, *asset* IT, dan ancaman siber. Seluruh landasan teori ini disusun untuk memberikan pemahaman konseptual yang komprehensif serta mendukung kerangka berpikir dalam penyusunan dan pelaksanaan penelitian

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metode konseptual yang digunakan dalam penelitian, yang mengacu pada *Information Systems Research Framework* sebagai dasar perancangan pendekatan ilmiah. Kerangka ini terdiri dari tiga komponen utama, yaitu *Environment*, IS *Research*, dan *Knowledge Base*, yang saling berkaitan satu sama lain dalam membentuk alur penelitian yang terstruktur. Pada komponen *Environment*, aspek yang dikaji mencakup *People, Organizations,* dan *Technology*, yang merepresentasikan konteks nyata dari objek penelitian, termasuk aktor yang terlibat, institusi yang dianalisis, serta teknologi yang digunakan. Komponen IS *Research* terdiri dari dua bagian utama, yaitu *Develop*/*Build* dan *Justify/Evaluate*, yang masing-masing menggambarkan proses konstruksi artefak penelitian serta evaluasi terhadap efektivitas pendekatan yang diterapkan. Sementara itu, *Knowledge Base* mencakup elemen *Foundations* dan *Methodologies*, yang berfungsi sebagai landasan teori dan metode untuk mendukung validitas dan keilmiahan dalam penelitian ini.

BAB IV EKSPERIMEN DAN DATA

Pada bab ini disajikan uraian mengenai data hasil *review* literatur, perencanaan dan persiapan eksperimen, serta penjelasan alur pelaksanaan eksperimen yang dilakukan. Bab ini juga memaparkan implementasi eksperimen berdasarkan masing-masing *tools* yang

digunakan, beserta penyajian data yang diperoleh dari eksplorasi terhadap *domain* layanan IT IKS menggunakan berbagai OSINT *tools*. Di akhir bab, disertakan pula ringkasan hasil eksperimen sebagai analisis lanjutan.

BAB V HASIL DAN EVALUASI

Pada bab ini disajikan uraian hasil analisis yang mencakup perumusan mulai dari definisi Aset Teknologi Informasi, penentuan Nilai Aset, identifikasi *Vulnerability* dan *Threat*, hingga pemetaan skenario ancaman berdasarkan perwakilan masing-masing IKS. Selanjutnya dilakukan perhitungan nilai risiko berdasarkan pendekatan kuantitatif, diikuti dengan proses klasterisasi tingkat risiko. Bab ini ditutup dengan ringkasan keseluruhan hasil analisis sebagai dasar penarikan kesimpulan.

BAB VI KESIMPULAN DAN SARAN

Pada bab ini disajikan kesimpulan dari keseluruhan hasil penelitian yang telah dilakukan, yang mencakup pemetaan risiko berbasis OSINT terhadap *domain* layanan IT IKS. Selain itu, disampaikan pula sejumlah saran yang dapat dijadikan bahan pertimbangan untuk penelitian selanjutnya.