BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong transformasi layanan IT institusi keuangan, termasuk pada institusi keuangan lokal yang dikelola pemerintah daerah. Dari yang awalnya berfokus pada pembiayaan mikro, kini institusi-institusi keuangan tersebut semakin mengandalkan infrastruktur teknologi informasi untuk mendukung operasional dan pelayanan. Namun, ketergantungan ini juga membuka potensi risiko serangan siber yang dapat mengancam stabilitas dan keberlangsungan sistem institusi keuangan. Kasus nyata yang menggambarkan risiko kerentanan pada sistem institusi keuangan terhadap serangan digital diungkap dalam penelitian, yang mengulas potensi ancaman pada institusi syariah di Indonesia menghadapi berbagai jenis serangan digital seperti *phishing, malware, ransomware*, hingga pencurian identitas, yang membuktikan bahwa institusi keuangan menjadi sasaran strategis dalam ranah serangan digital (Abdullah Mubarak Lubis et al., 2025).

Dalam tahap awal eksplorasi penelitian, dilakukan perbandingan terhadap objek yang akan diteliti yakni beberapa jenis *domain* situs pemerintahan dan *platform event management* yang berguna untuk menilai sejauh mana potensi risiko dan paparan layanan IT dapat dianalisis menggunakan pendekatan OSINT. Namun, hasil analisis menunjukkan bahwa risiko pada objek-objek tersebut tidak menunjukkan eksposur yang signifikan secara fungsional. Sementara itu, sektor keuangan lokal, memiliki karakteristik aset digital yang lebih krusial, seperti *domain* layanan IT, layanan transaksi berbasis web, serta sistem informasi yang menangani data sensitif dan informasi keuangan. Hal ini menjadikan institusi institusi keuangan lokal sebagai objek yang lebih memiliki dampak dalam konteks analisis risiko siber berbasis domain publik.

Open-Source Intelligence (OSINT) menjadi pendekatan yang relevan untuk tujuan tersebut. OSINT diperkirakan menyumbang 70-90% dari total informasi intelijen saat ini (Ghioni et al., 2024). Karena sifatnya yang non-intrusif, metode ini sangat

cocok digunakan untuk menilai risiko pada institusi dengan berbagai ancaman siber, tanpa memerlukan akses ke sistem internal. (Puyvelde & Rienzi, 2025).

Penelitian ini memanfaatkan OSINT untuk menyusun estimasi risiko siber pada *domain-domain* milik institusi keuangan lokal, dengan pendekatan kuantitatif berbasis model *CRAMM* (*CCTA Risk Analysis and Management Method)*. Nilai aset diperkirakan dari klasifikasi layanan IT berdasarkan publikasi keuangan nasional yang dirilis pada awal tahun 2025, sementara kerentanan dan ancaman dipetakan menggunakan *tools* OSINT. Dengan pendekatan ini, penelitian diharapkan mampu memberikan gambaran awal mengenai estimasi tingkat risiko siber pada Institusi Keuangan Lokal dari sudut pandang eksternal berbasis OSINT. Temuan ini nantinya bertujuan untuk memahami distribusi eksposur risiko, serta mengaitkannya dengan estimasi nilai aset IT secara komparatif yang dimiliki oleh masing-masing institusi.

I.2 Perumusan Masalah

1. Bagaimana profil risiko pada layanan teknologi informasi milik institusi Institusi Keuangan Lokal dapat diidentifikasi melalui teknik *Passive Preliminary Surveillance*?
2. Bagaimana fungsi OSINT terhadap *domain* Institusi Keuangan Lokal dapat memberikan gambaran potensi ancaman yang dihadapi?
3. Bagaimana proses perumusan risiko dapat dilakukan berdasarkan temuan kerentanan dan ancaman dari hasil observasi OSINT?

I.3 Tujuan Penelitian

1. Identifikasi profil estimasi risiko pada *domain* terbuka milik Institusi Keuangan Lokal melalui analisis pendekatan OSINT menggunakan teknik *Passive Preliminary Surveillance*.
2. Analisis fungsi OSINT berdasarkan kerentanan, dan potensi ancaman, menggunakan model *Data Flow Diagram* dan *Attack Tree* untuk melihat berapa besar risiko ancaman dapat terjadi dari temuan yang didapatkan.
3. Perumusan estimasi risiko berdasarkan hasil temuan kerentanan dan potensi ancaman yang terdeteksi dari data terbuka, dengan menggabungkan nilai

aset institusi, jumlah kerentanan, dan potensi ancaman menggunakan formula kuantitatif berbasis pendekatan CRAMM.

I.4 Batasan Penelitian

1. Penelitian ini hanya menggunakan teknik pengumpulan data berbasis OSINT dan tidak mencakup akses internal atau uji coba langsung terhadap sistem target
2. Kerentanan dan ancaman yang dikaji bersifat potensial, serta tidak semua ancaman dapat divalidasi secara nyata karena keterbatasan akses terhadap sistem internal.
3. Penelitian ini dibatasi pada analisis terhadap *domain* resmi milik Institusi Keuangan Lokal, tanpa melibatkan analisis terhadap layanan tertentu seperti *mobile institusiing, internet institusiing*, maupun sistem internal lainnya yang tidak secara langsung berkaitan dengan *domain* utama.

I.5 Manfaat Penelitian

1. Secara Teoritis
   a. Menambah wawasan mengenai penerapan *Open-Source Intelligence* (OSINT) dalam proses identifikasi dan estimasi risiko terhadap layanan teknologi informasi, khususnya pada institusi keuangan daerah.
   b. Memahami bagaimana kerangka penilaian risiko berbasis OSINT dapat dirumuskan melalui integrasi antara data aset layanan IT, kerentanan, dan potensi ancaman yang terdeteksi secara terbuka.
2. Secara Praktis
   a. Mengetahui fungsi praktis dari berbagai *tools* OSINT dalam mendeteksi dan memetakan titik-titik kerentanan layanan IT, serta bagaimana informasi tersebut dapat diolah menjadi dasar perumusan estimasi risiko.
   b. Menghasilkan dokumentasi informasi yang terstruktur mengenai proses pengumpulan data OSINT, visualisasi model serangan yakni *Data Flow Diagram* dan *Attack Tree*, serta klasifikasi risiko keamanan layanan TI suatu institusi.

I.6 Sistematika Penulisan

Struktur penulisan dalam penelitian ini disusun dengan sistematika sebagai Berikut:

BAB I PENDAHULUAN

Bab ini berisikan perumusan masalah terkait bagaimana pendekatan *Open-Source Intelligence* (OSINT) dapat dimanfaatkan untuk mengidentifikasi dan merumuskan estimasi tingkat risiko siber terhadap layanan teknologi informasi milik Institusi Keuangan Lokal, khususnya dari sudut pandang eksternal. Penelitian ini bertujuan untuk memberikan gambaran awal mengenai potensi kerentanan dan ancaman yang dapat terdeteksi melalui observasi terbuka menggunakan teknik *Passive Preliminary Surveillance*. Fokus utama dalam penelitian ini adalah merumuskan estimasi tingkat risiko siber terhadap *domain* pada Institusi Keuangan Lokal berdasarkan temuan nilai aset layanan IT, kerentanan, serta potensi ancaman yang teridentifikasi secara terbuka. Pendekatan ini dilakukan dengan mengadopsi metode kuantitatif melalui pendekatan CRAMM (*CCTA Risk Analysis and Management Method)* berdasarkan pendekatan dijelaskan oleh Darril Gibson dalam bukunya *Managing Risk in Information Systems*.

Adapun ruang lingkup penelitian ini dibatasi pada tahap pengumpulan informasi yang bersifat pasif tanpa intervensi terhadap sistem target, serta tidak melibatkan proses eksploitasi atau pengujian langsung terhadap infrastruktur internal Institusi Keuangan Lokal. Penelitian ini hanya berfokus pada proses identifikasi risiko berbasis data terbuka dan tidak mencakup perumusan strategi mitigasi atau penanganan risiko secara langsung.

BAB II TINJAUAN PUSTAKA

Bab ini berisi teori dan literatur yang relevan dengan topik penelitian mengenai implementasi dan analisis *profiling* terhadap ancaman siber berbasis *Open-Source Intelligence* (OSINT) dalam konteks

keamanan informasi di lembaga keuangan Institusi Keuangan Lokal. Adapun konsep-konsep utama yang dibahas mencakup Data Publik, Ancaman Siber, *Open-Source Intelligence* (OSINT), *Profiling* Risiko, Aset IT, *Preliminary Surveillance*, *Threat Modeling, Data Flow Diagram,* serta *Attack Tree* yang kerap menyasar institusi keuangan, yang akan digunakan sebagai landasan untuk mendukung pembahasan penelitian mengenai *profiling* estimasi risiko ancaman siber berdasarkan OSINT.

BAB III METODOLOGI PENELITIAN

Bab ini membahas metode konseptual yang meliputi tiga komponen utama, yaitu *Environment*, *IS Research*, dan *Knowledge Base*. Pada bagian *Environment* mencakup tiga elemen utama, yaitu *People, Organization* dan *Technology.* Kemudian, pada bagian *IS Research*, fokusnya adalah pada proses *develop/build* dan *justify/evaluate*. Sementara itu, bagian *Knowledge Base* mencakup aspek *foundations* dan *methodologies*. Selain itu, bab ini juga menjelaskan sistematika penyelesaian masalah yang disusun dalam enam tahapan, yaitu tahap awal, tahap hipotesis, tahap desain, tahap eksperimen, analisis hasil, dan tahap akhir.

BAB IV PERANCANGAN DAN ALUR EKSPERIMEN

Bab ini menjelaskan tahapan-tahapan dalam pelaksanaan eksperimen yang dimulai dari penjelasan Data *Review* Literatur, selanjutnya tahap perencanaan dan persiapan eksperimen berupa, Spesifikasi Perangkat Keras, Spesifikasi Perangkat Lunak, Daftar target *domain* yang digunakan, kemudian alur eksperimen, implementasi eksperimen, data hasil eksperimen, dan ringkasan data eksperimen dari proses pemindaian informasi publik yang tersedia dari aset layanan IT menggunakan *tools* OSINT dari masing-masing *domain*.

BAB V ANALISIS

Bab ini berisi analisis terhadap hasil observasi menggunakan pendekatan *Open-Source Intelligence* (OSINT) untuk memetakan estimasi risiko keamanan informasi pada lima belas Institusi Keuangan Lokal milik pemerintah daerah. Analisis dimulai dengan perumusan definisi aset teknologi informasi dan penilaian nilai aset (A), dilanjutkan dengan identifikasi tingkat kerentanan (V) berdasarkan temuan teknis dari berbagai *tools* OSINT, serta pemetaan skenario ancaman potensial (T) yang dirumuskan secara hipotetis dari data observasi. Selanjutnya, dilakukan visualisasi model serangan dalam bentuk *Data Flow Diagram* (DFD) *dan Attack Tree* pada empat jenis serangan utama, yaitu *Man-in-the-Middle, DNS Hijacking*, dan *Brute Force Login*. Nilai risiko akhir (R) dihitung menggunakan rumus R = V × T × A, kemudian diklasifikasikan ke dalam kategori risiko tinggi, sedang, dan rendah menggunakan metode *equal-width interval*. Pada bab ini juga disajikan analisis perbandingan estimasi risiko antar institusi keuangan lokal untuk mengidentifikasi prioritas penguatan keamanan TI berdasarkan eksposur aset IT dan potensi ancaman yang terdeteksi.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi ringkasan hasil dari seluruh proses penelitian yang telah dilaksanakan. Selain itu, dalam bab ini juga disampaikan sejumlah saran yang diharapkan dapat menjadi acuan atau masukan untuk pengembangan penelitian untuk penelitian selanjutnya.