BAB I PENDAHULUAN

I.1 Latar Belakang

Digitalisasi telah menjadi fondasi utama dalam pengembangan layanan publik dan ekonomi di era modern. Sektor jasa keuangan, sebagai salah satu pilar sistem perekonomian nasional dan regional, berada di garis depan transformasi ini. Pada tingkat regional, institusi keuangan regional memainkan peran penting dalam menyediakan akses layanan keuangan digital bagi masyarakat dan pemerintah daerah. Namun, perluasan infrastruktur teknologi informasi dapat memperluas *attack surface* dan memunculkan potensi risiko dari luar sistem. Hal ini diperkuat dari laporan *Data Breach Investigations Report* (DBIR) 2024 yang mencatat 3.348 insiden keamanan di sektor keuangan, di mana serangan kompleks umumnya diawali dengan *passive reconnaissance* (Verizon Business, 2024).

Menyikapi tantangan tersebut, dibutuhkan pendekatan intelijen yang memanfaatkan informasi dari sumber terbuka, yang dikenal sebagai *Open-Source Intelligence*. OSINT didefinisikan sebagai proses pengumpulan dan analisis data dari sumber-sumber terbuka yang dapat diakses publik (Bazzell, 2023). Studi kasus di sektor keuangan menunjukkan efektivitas OSINT dalam mengungkap informasi sensitif karyawan untuk mendukung pengelolaan kerentanan institusi (Rajamäki & Tiitta, 2024). Namun, pendekatan ini masih didominasi metode kualitatif yang bergantung pada interpretasi analis, sehingga penilaian risiko sulit dikuantifikasi dan direplikasi secara konsisten (Van Puyvelde & Tabárez Rienzi, 2025).

Sebagai solusi atas celah metodologis tersebut, penelitian ini menerapkan *framework* kuantitatif yang sistematis dengan mengadaptasi alur kerja dari metodologi *CCTA Risk Analysis and Management Methodology* (CRAMM) dimana $Risk = Vulnerabillity \times Threat \times Asset$ (Yazar, 2000). Setiap variabel dalam model ini diberi skor numerik berdasarkan data yang diperoleh melalui teknik *passive reconnaissance* berbasis OSINT serta data sekunder yang tersedia secara publik. Dengan demikian, pendekatan ini mentransformasi temuan OSINT yang

semula kualitatif menjadi skor risiko kuantitatif, memungkinkan penyusunan profil risiko yang objektif dan komparatif bagi setiap Institusi Keuangan Regional.

I.2 Perumusan Masalah

Sejalan dengan uraian pada latar belakang, permasalahan yang diangkat dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana *Vulnerability* potensial pada layanan IT Institusi Keuangan Regional dapat diidentifikasi?
2. Bagaimana temuan kerentanan dapat dimodelkan menjadi skenario serangan untuk memvisualisasikan potensi jalur eksploitasi?
3. Bagaimana profil risiko pada layanan IT masing-masing Institusi Keuangan Regional?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan sebelumnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi *Vulnerability* pada layanan IT Institusi Keuangan Regional dengan memanfaatkan pendekatan OSINT melalui teknik *passive reconnaissance*.
2. Mengembangkan model skenario Ancaman yang didasarkan pada temuan *Vulnerability* (V), dengan menggunakan *Data Flow Diagram* dan *Attack Tree* untuk memvisualisasikan jalur eksploitasi.
3. Menyusun profil estimasi risiko layanan IT masing-masing Institusi Keuangan Regional dalam bentuk peringkat komparatif dengan mengintegrasikan skor kuantitatif *Vulnerability* (V), *Threat* (T), dan *Asset* (A) ke dalam formula $R = V \times T \times A$.

I.4 Batasan Penelitian

Adapun batasan penelitian pada penelitian ini sebagai berikut:

1. Penelitian bersifat non-intrusif menggunakan OSINT *Tools* pada *domain* publik resmi Institusi Keuangan Regional, tidak mencakup sistem internal atau yang memerlukan otentikasi.

2. Penilaian variabel *Vulnerabillity* (V) dan *Threat* (T) didasarkan pada jumlah temuan (*count-based*), dan tidak menggunakan pembobotan berdasarkan tingkat keparahan (*severity*).
3. Model skenario serangan yang disusun dalam penelitian ini bersifat konseptual dan disajikan sebagai bentuk *Proof of Concept* berbasis analisis.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian tugas akhir ini adalah sebagai berikut:

1. Secara teoritis
   a. Mengembangkan dan memvalidasi sebuah kerangka kerja kuantitatif berbasis OSINT, dengan menggunakan pendekatan model estimasi risiko dirancang berdasarkan kerangka kerja analisis risiko dari CRAMM, untuk mengukur risiko layanan internet dari perspektif eksternal.
   b. Memberikan kontribusi terhadap literatur terkait *threat modeling* melalui penerapan visualisasi serangan berbasis *Data Flow Diagram* dan *Attack Tree*.
2. Secara praktis
   a. Menyediakan penggunaan praktis dari berbagai OSINT *Tools* dan teknik *passive reconnaissance* untuk melakukan identifikasi kerentanan pada layanan IT Institusi Keuangan Regional.
   b. Menyediakan panduan metodologis mengenai praktik penyusunan potensi *Threat* yang logis, yang didasarkan langsung pada temuan *Vulnerability*.

I.6 Sistematika Penulisan

Penelitian ini disusun secara sistematis dalam enam bab, dengan rincian sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas latar belakang, perumusan masalah, tujuan, manfaat, batasan penelitian, serta sistematika penulisan. Pembahasan diawali dengan urgensi pengelolaan risiko pada layanan Internet yang dihadapi Institusi Keuangan Regional, termasuk tantangan

akibat meningkatnya eksposur sistem ke ruang publik. Bab ini juga mengkritisi keterbatasan pendekatan yang ada, serta menerapkan model kuantitatif untuk estimasi risiko layanan Internet berbasis OSINT dengan mengadaptasi alur kerja dari metodologi CRAMM.

BAB II TINJAUAN PUSTAKA

Bab ini menyajikan teori-teori yang mencakup konsep dasar OSINT, kerangka kerja estimasi risiko yang diadaptasi dari CRAMM, beserta definisi dari setiap komponennya: *Vulnerability, Threat,* dan *Asset*, serta pendekatan *Threat Modeling* yang digunakan untuk menganalisis potensi serangan terhadap sistem informasi. Selain itu, dijelaskan pula metode visualisasi skenario serangan menggunakan *Data Flow Diagram* dan *Attack Tree*. Penjelasan ini dilengkapi dengan justifikasi pemilihan kerangka kerja dan perbandingan dengan penelitian terdahulu untuk menunjukkan kebaruan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini memaparkan secara rinci metodologi penelitian yang dibingkai dalam paradigma *Design Science Research*. Pembahasan mencakup perancangan model konseptual dan sistematika penyelesaian masalah yang menjadi panduan alur kerja. Bab ini juga menjelaskan strategi pengumpulan data menggunakan teknik *passive reconnaissance* berbasis OSINT, pemodelan skenario serangan berdasarkan kerentanan, perumusan model kuantitatif serta metode evaluasi untuk mengklasifikasikan skor risiko.

BAB IV EKSPERIMEN DAN DATA

Bab ini menyajikan secara rinci tahapan implementasi eksperimen pengumpulan data. Pembahasan diawali dengan penentuan sumber data dan *domain* target, diikuti oleh perencanaan teknis lingkungan eksperimen. Selanjutnya, diuraikan alur dan implementasi untuk setiap OSINT *Tools* yang digunakan serta disajikan data temuan hasil eksperimen.

BAB V ANALISIS

Bab ini membahas proses analisis terhadap data hasil eksperimen yang telah dikumpulkan, dengan fokus pada perhitungan nilai *Asset* (A), *Vulnerability* (V), dan *Threat* (T) untuk menghasilkan estimasi risiko. Selain analisis kuantitatif, bab ini juga menyajikan pemodelan skenario serangan menggunakan DFD dan *Attack Tree* untuk memperlihatkan kemungkinan jalur eksploitasi terhadap *domain* yang dianalisis. Hasil akhir digunakan untuk membandingkan tingkat estimasi risiko layanan internet antar Institusi Keuangan Regional secara lebih terstruktur.

BAB VI KESIMPULAN DAN SARAN

Bab ini merupakan bagian penutup yang menyajikan dua komponen utama. Pertama, kesimpulan yang secara ringkas menjawab setiap rumusan masalah penelitian, mulai dari proses identifikasi kerentanan, pemetaan ancaman, hingga hasil akhir dari profil estimasi risiko kuantitatif yang telah disusun. Kedua, saran yang diajukan berdasarkan temuan dan keterbatasan penelitian, yang ditujukan untuk pengembangan riset di masa mendatang maupun untuk pertimbangan praktis bagi pihak terkait.