IMPLEMENTASI DAN ANALISIS *INFORMATION GATHERING* MENGGUNAKAN *OPEN-SOURCE INTELLIGENCE* (OSINT) *TOOLS* UNTUK ESTIMASI RISIKO PADA LAYANAN IT INSTITUSI KEUANGAN SYARIAH

1st Rhoemanidar Ruslan
Sistem Informasi
Fakultas Rekayasa Industri
Bandung, Indonesia
rhoemanidarrm@student.telkomuniversity.ac.id

2nd Adityas Widjajarto, S.T., M.T.
Sistem Informasi
Fakultas Rekayasa Industri
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd Umar Yunan Kurnia Septo Hediyanto, S.T., M.T.
Sistem Informasi
Fakultas Rekayasa Industri
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

***Abstrak* — Perkembangan layanan teknologi informasi di sektor keuangan mendorong Institusi Keuangan Syariah mengadopsi sistem berbasis *website* untuk efisiensi, namun kesiapan keamanan informasi masih terbatas. IKS menghadapi tantangan sumber daya, infrastruktur, dan kapabilitas dalam mendeteksi serta mengelola risiko siber, terutama dengan meningkatnya serangan yang mengeksploitasi celah digital. Oleh karena itu, penelitian ini bertujuan merumuskan estimasi risiko berbasis *Open-Source Intelligence* (OSINT) untuk menilai kerentanan dan ancaman siber terhadap aset IT IKS secara eksternal. Metode penelitian meliputi identifikasi *domain* IKS dari Publikasi Nasional, eksplorasi *domain* menggunakan *tools* OSINT untuk data teknis seperti *port* terbuka dan konfigurasi SSL, serta analisis risiko dengan model R=V×T×A. Hasil menunjukkan sebagian besar *domain* IKS memiliki kerentanan pada infrastruktur dan layanan dasar, seperti sertifikat SSL dan pengaturan email yang terbuka, serta menampilkan informasi sensitif. Ancaman umum bersumber dari eksploitasi pasif informasi publik. Melalui model risiko, IKS diklasifikasikan ke dalam tiga tingkat risiko (tinggi, sedang, rendah), menunjukkan bahwa setiap *domain* memiliki potensi ancaman siber yang perlu diwaspadai. Pendekatan OSINT terbukti mampu memberikan gambaran awal kondisi keamanan IT IKS, bermanfaat sebagai dasar evaluasi mandiri dan rekomendasi perbaikan sistem, serta berkontribusi pada pengembangan strategi pertahanan siber efisien berbasis informasi terbuka untuk sektor keuangan lokal.**

***Kata kunci*— Keamanan informasi IKS, *open-source intelligence* (OSINT), estimasi risiko siber, kerentanan sistem**

I. PENDAHULUAN

Di era digital saat ini, di mana informasi mengalir secara terbuka dan mudah diakses, *Open-Source Intelligence* (OSINT) hadir memainkan peran penting sebagai sumber informasi terbuka yang digunakan dalam berbagai operasi siber. Menurut Khera [1], OSINT melibatkan pengumpulan informasi dari sumber-sumber yang 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, ancaman siber merujuk pada segala kondisi, situasi, atau kemampuan yang berpotensi menimbulkan gangguan dan serangan yang dapat merusak serta menimbulkan kerugian. Ancaman ini mencakup kepada potensi risiko kerahasiaan, ketersediaan, dan integritas suatu sistem maupun informasi. Dalam konteks ini, ancaman yang dimaksud belum tentu terjadi tetapi memiliki potensi untuk menyebabkan kerugian (*risk*). Karakteristik serangan siber umumnya melibatkan perangkat digital sebagai alat utama, dengan konsekuensi yang berdampak pada sistem elektronik, bukan pada infrastruktur fisik secara langsung [2].

Salah satu sektor yang sangat rentan terhadap ancaman siber adalah sektor perbankan. Keamanan siber dalam perbankan menjadi isu yang semakin krusial seiring pesatnya digitalisasi layanan keuangan. Perbankan modern kini sangat bergantung pada sistem digital untuk mendukung layanan kepada nasabah, mulai dari transaksi daring hingga pengelolaan data sensitif. Namun, ketergantungan ini juga meningkatkan eksposur terhadap potensi serangan siber, terutama apabila terdapat informasi terbuka yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Serangan seperti pencurian data pribadi, peretasan sistem layanan, dan penyalahgunaan akses administratif telah menyebabkan kerugian besar di berbagai institusi keuangan di dunia [3]. Menurut laporan IBM X-Force *Threat* Intelligence Index 2024, sektor keuangan dan asuransi menempati posisi teratas sebagai industri yang paling banyak diserang secara global selama tiga tahun berturut-turut, dengan 18,9% dari total insiden siber pada tahun 2023 menargetkan sektor ini [4].

Di Indonesia sendiri, data dari Lanskap Keamanan Siber Indonesia 2024 yang dirilis oleh BSSN menunjukkan bahwa

sektor keuangan masih tergolong sebagai sektor prioritas dalam ancaman siber nasional. Sepanjang tahun 2024, tercatat sebanyak 9 dugaan insiden yang menyerang sektor ini, dengan proporsi 3,58% dari total 56.128.160 temuan data *exposure* yang berasal dari institusi keuangan [5]. Meskipun secara persentase lebih kecil dibanding sektor pemerintahan, temuan ini tetap menunjukkan bahwa sektor keuangan memiliki tingkat risiko yang tinggi mengingat karakteristik datanya yang sensitif dan bernilai ekonomis.

Temuan data tersebut memberikan gambaran bahwa sektor keuangan merupakan salah satu sektor yang strategis namun memiliki tingkat kerentanan tinggi terhadap ancaman siber. Tingginya digitalisasi layanan keuangan dan nilai kritis dari data yang dikelola menjadikan sektor ini sebagai sasaran yang menarik bagi pelaku serangan. Meski tidak menempati jumlah insiden tertinggi, keberadaan data *exposure* serta dugaan insiden yang tercatat menunjukkan adanya celah keamanan yang tidak dapat diabaikan.

Dalam konteks inilah, penelitian ini difokuskan pada sektor Institusi Keuangan Syariah, dengan pemanfaatan data publik dari Publikasi Nasional sebagai dasar dalam mengidentifikasi aset digital. Aset dalam penelitian ini tidak merujuk pada infrastruktur internal perbankan yang tidak dapat diakses secara terbuka, melainkan diestimasi berdasarkan nilai aset lembaga yang tercatat dalam publikasi Publikasi Nasional, sebagai representasi tingkat kepentingan dan nilai strategis dari setiap institusi. Dalam hal ini, pendekatan OSINT digunakan sebagai alat untuk menghimpun informasi terbuka terkait potensi kerentanan dan eksposur digital dari masing-masing *domain* IKS, sehingga memungkinkan analisis risiko dapat dilakukan tanpa bergantung pada akses langsung ke sistem internal perbankan.

II. KAJIAN TEORI

A. Data Publik

Data publik adalah informasi yang dapat dibagikan, digunakan, digunakan kembali, dan didistribusikan ulang tanpa batasan. Data ini mencakup berbagai format dan ukuran, seperti kumpulan data dan statistik, serta data yang telah terstruktur dan diolah maupun data mentah yang belum terstruktur. Data publik biasanya disimpan dan diakses melalui situs web perusahaan atau pemerintah, serta disimpan oleh perusahaan dan penyedia data lainnya [6].

B. *Risk Assestment*

Risk Assessment adalah proses penting dalam manajemen keamanan informasi untuk mengidentifikasi, menganalisis, dan mengevaluasi ancaman serta kerentanan yang berpotensi merugikan aset. Tujuannya adalah untuk menentukan seberapa besar risiko yang ada dan menjadi dasar dalam membuat strategi mitigasi yang efektif [7].

C. *Open-Source Intelligence* (OSINT)

Istilah *Open-Source Intelligence* (OSINT) awalnya mengacu kepada sumber tertentu dari intelijen. Secara umum, sumber intelijen digunakan untuk menghasilkan data mentah yang nantinya dapat diolah lebih lanjut melalui enam tahap dalam siklus intelijen untuk mendapatkan wawasan. OSINT didefinisikan sebagai intelijen yang dihasilkan dari sumber-sumber yang tersedia untuk umum, yang dikumpulkan, dimanfaatkan, dan disebarluaskan secara tepat waktu kepada audiens yang sesuai untuk memenuhi kebutuhan intelijen tertentu [8].

D. *Information Gathering*

Dalam dunia keamanan siber, *information gathering* adalah proses mendapatkan data apa pun. Ini merupakan fase awal dan sangat penting dalam peretasan secara etis, yang dilakukan oleh penester atau peretas. Semakin banyak data yang terkumpul tentang target, semakin tinggi peluang keberhasilan. Pengumpulan informasi bukan hanya langkah dalam pengujian penetrasi, melainkan kemampuan vital yang harus dikuasai setiap penester dan peretas untuk mencapai hasil penetrasi yang lebih baik [9].

E. *Cyber Profiling*

Cyber Profiling adalah metode psikologis dan kriminologi yang berfungsi untuk mengidentifikasi kecenderungan perilaku, ciri-ciri pribadi, dan demografi pelaku kejahatan siber guna memprediksi aktivitas kriminal mereka. Ini merupakan bidang interdisipliner yang terus berkembang dalam kriminologi. Profil ini menggabungkan karakteristik personal, pola perilaku, dan data demografi berdasarkan kejahatan siber yang dilakukan. Prosesnya melibatkan analisis aspek korban, klarifikasi motif, identifikasi ciri-ciri pelaku, dan analisis perilaku digital atau bukti digital [10]

F. *Threat Modelling*

Pemodelan ancaman adalah proses terstruktur untuk mengidentifikasi potensi kerentanan dan ancaman keamanan, mengevaluasi tingkat keparahan risiko, serta memprioritaskan langkah perlindungan untuk meminimalkan serangan pada infrastruktur. Ini membantu mengidentifikasi dan menilai ancaman yang dapat memengaruhi sistem secara sistematis. Proses ini umumnya dibagi menjadi tiga langkah utama: dekomposisi aplikasi, klasifikasi ancaman, dan penentuan tindakan pencegahan untuk mengurangi risiko [11].

G. *Asset* IT

Dalam konteks bisnis, aset merujuk pada segala sesuatu yang memiliki nilai tukar, mencakup baik modal maupun kekayaan. Aset bisa berwujud fisik seperti benda atau bangunan, atau non-fisik seperti uang. Secara lebih spesifik, aset IT diartikan sebagai kekayaan perusahaan dalam bentuk *hardware* dan *software*. Penting untuk diingat bahwa aset IT ini harus dikelola dengan baik, dioptimalkan penggunaannya, dan dijamin keamanannya agar dapat secara efektif mendukung pencapaian tujuan suatu instansi atau perusahaan dalam menjalankan operasional bisnis mereka [12].

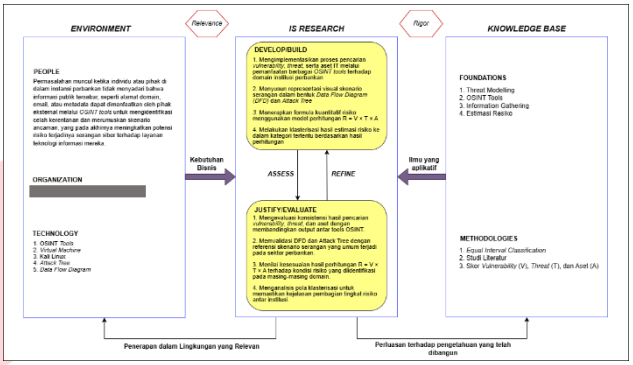
H. Ancaman Siber

Ancaman siber, yang meliputi pencurian data, serangan malware, dan serangan *Distributed Denial of Service* (DDoS), merupakan isu krusial dalam keamanan digital. Guna membangun komunitas keamanan siber yang tangguh, kolaborasi antarnegara dan implementasi strategi pengamanan siber yang terpadu menjadi esensial. Strategi ini mencakup peningkatan kapasitas sumber daya manusia dan teknologi, pembentukan sistem pertahanan dan keamanan berbasis siber yang adaptif, serta kerja sama teknis dan sinergi antara berbagai pihak. Studi mendalam mengenai pengamanan siber sangat penting untuk memperkaya pemahaman tentang tipologi serangan siber, taktik yang digunakan oleh aktor ancaman, dan mengidentifikasi kerentanan sistem yang ada [13].

III. METODE

A. Model Konseptual

Model konseptual berfungsi sebagai kerangka sistematis untuk menggambarkan keterkaitan antar konsep yang relevan dalam suatu bidang studi. Model ini mengilustrasikan fenomena yang dikaji melalui representasi konsep-konsep kunci, baik berupa gagasan abstrak maupun entitas konkret, yang membentuk dasar pemahaman terhadap isu yang diteliti. Visualisasi berikut merepresentasikan hubungan logis dari elemen-elemen utama dalam penelitian ini.

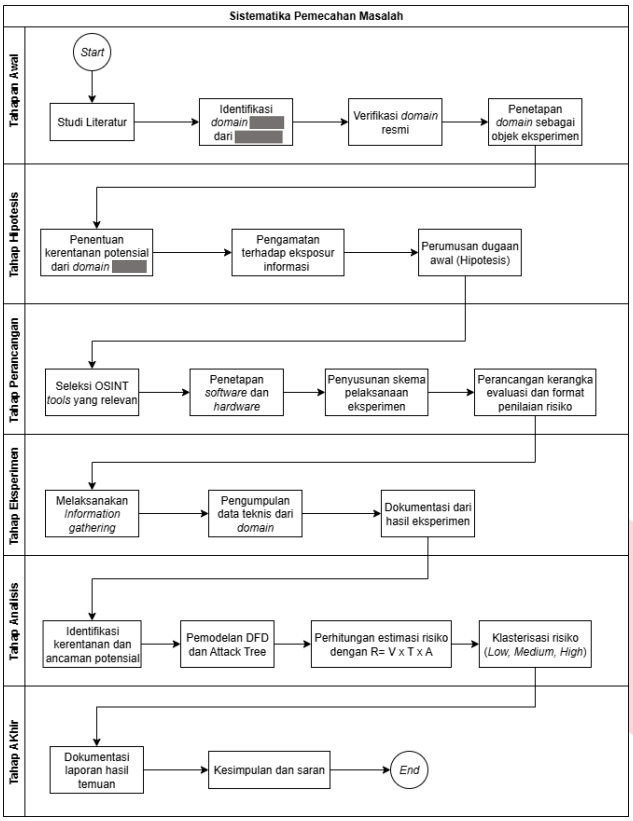


Gambar 1. *Information Systems Research Framework*

Berdasarkan diagram di atas, penelitian ini mengusung kerangka kerja yang komprehensif untuk penilaian risiko keamanan informasi, memadukan elemen-elemen lingkungan (*People, Organization, Technology*), metodologi penelitian sistem informasi (*Develop/Build, Assess, Refine, Justify/Evaluate*), dan basis pengetahuan (*Foundations, Methodologies*). Pendekatan ini secara khusus menyoroti penggunaan OSINT *tools* dan teknik seperti DFD (*Data Flow Diagram*) serta *Attack Tree* untuk mengidentifikasi dan memitigasi kerentanan, serta menghitung estimasi risiko.

B. Sistematika Penyelesaian Masalah

Penelitian ini mengadopsi sistematika penyelesaian masalah yang terstruktur, mencakup enam fase krusial. Dimulai dengan tahap perencanaan awal untuk mengidentifikasi isu dan merumuskan asumsi dasar, proses ini berlanjut ke pengajuan hipotesis. Selanjutnya, fase perancangan melibatkan desain alat dan alur eksperimen yang akan digunakan. Tahap pelaksanaan eksperimen fokus pada pengumpulan data, yang kemudian dianalisis secara mendalam pada fase analisis data guna mengevaluasi hipotesis yang telah diajukan. Akhirnya, tahap penyelesaian akhir mencakup penyusunan laporan komprehensif berisi temuan, kesimpulan, dan rekomendasi dari penelitian ini.



Gambar 2 Sistematika penyelesaian masalah

Diagram di atas menyajikan alur sistematis penyelesaian masalah dalam penelitian ini, terbagi menjadi enam tahapan utama. Dimulai dengan Tahap Awal, penelitian melakukan studi literatur untuk mengidentifikasi dan menganalisis keterbukaan informasi pada *domain* IKS yang dapat dimanfaatkan dari pihak eksternal berbasis OSINT. Tahap Hipotesis melibatkan pengumpulan jenis OSINT *tools* dan perumusan dugaan awal. Selanjutnya, Tahap Perancangan fokus pada penentuan OSINT *tools* yang relevan, spesifikasi *hardware* dan *software*, pengembangan skema eksperimen, serta penyusunan kriteria evaluasi dan kerangka penilaian risiko. Pada Tahap Eksperimen, data atau informasi publik dikumpulkan, kemampuan deteksi OSINT diuji, dan hasilnya dicatat. Tahap Analisis mencakup inventarisasi kerentanan, identifikasi ancaman, penilaian aset IT, perhitungan risiko dengan formula, dan klasterisasi *domain* berdasarkan tingkat risiko. Terakhir, Tahap Akhir melibatkan dokumentasi laporan, penarikan kesimpulan, dan pemberian saran.

IV. HASIL DAN PEMBAHASAN

A. Penentuan Kuantifiasi Nilai Aset

Untuk memberikan bobot kuantitatif pada nilai aset (A), penelitian ini mengklasifikasikan aset institusi berdasarkan total aset yang dianalisis. Rentang kategorisasi disesuaikan dengan karakteristik dan skala Institusi Keuangan Syariah yang menjadi objek studi. Penilaian ini bertujuan untuk mencerminkan nilai strategis institusi, yang diasumsikan berbanding lurus dengan skala dan kompleksitas aset teknologi informasi yang digunakan. Setiap kategori aset diberikan skor antara 1 hingga 5, di mana skor tertinggi menunjukkan aset terbesar. Skor yang dihasilkan ini kemudian digunakan sebagai komponen kunci dalam perhitungan risiko pada tahap akhir analisis.

Tabel 1. Rentang skor aset

No.	Nama IKS	Kategori Aset	Skor A
1	Institusi Keuangan Syariah A	≥ Rp 250 Miliar	5
2	Institusi Keuangan Syariah B		
3	Institusi Keuangan Syariah C	Rp 100 Miliar – < Rp 250 Miliar	3
4	Institusi Keuangan Syariah D		
5	Institusi Keuangan Syariah E		
6	Institusi Keuangan Syariah F	Rp 50 Miliar – < Rp 100 Miliar	2
7	Institusi Keuangan Syariah G		
8	Institusi Keuangan Syariah H		

Skor yang disajikan dalam tabel mengklasifikasikan nilai aset dari setiap bank yang diteliti. Semakin tinggi skor yang diperoleh, semakin besar pula estimasi nilai dan kompleksitas aset teknologi informasi yang dimiliki institusi tersebut. Skor ini selanjutnya akan diintegrasikan sebagai salah satu variabel dalam proses analisis risiko pada tahap berikutnya.

B. Penentuan Kuantifikasi Nilai Kerentanan (V)

Dalam bagian ini, kami merumuskan nilai kerentanan untuk setiap institusi IKS. Penilaian ini didasarkan pada data yang dikumpulkan melalui eksplorasi mendalam menggunakan beragam alat OSINT. Tujuan utama dari penilaian ini adalah untuk mengukur secara kuantitatif tingkat kerentanan sistem informasi yang dimiliki oleh masing-masing institusi, sekaligus memahami sejauh mana sistem tersebut terekspos terhadap potensi gangguan atau serangan siber. Nilai kerentanan (V) yang diperoleh ini akan menjadi fondasi awal dalam menyusun analisis risiko yang lebih komprehensif, yang pada tahap selanjutnya akan diintegrasikan dengan parameter Ancaman (T) dan Aset (A).

Proses penilaian kerentanan dilakukan secara kuantitatif dengan menjumlahkan setiap temuan kelemahan dari berbagai hasil pengujian OSINT. Suatu temuan secara spesifik dikategorikan sebagai kerentanan apabila mengindikasikan adanya potensi kelemahan pada sistem yang dapat dieksploitasi oleh pihak yang tidak berwenang. Kriteria utama untuk pengkategorian kerentanan ini meliputi: (1) terbukanya layanan jaringan yang tidak dilindungi atau menggunakan protokol yang tidak aman; (2) ditemukannya akses terhadap berkas atau direktori yang bersifat sensitif atau tersembunyi; (3) teridentifikasinya penggunaan perangkat lunak dengan versi lama atau yang sudah tidak lagi didukung oleh pengembang; (4) terbukanya antarmuka sub*domain* yang berkaitan dengan fungsi administratif atau operasional internal; dan (5) ditemukannya kelemahan dalam konfigurasi keamanan web, seperti tidak adanya kebijakan keamanan HTTP yang memadai atau penggunaan sertifikat SSL yang tidak dapat diverifikasi. Setiap temuan yang memenuhi kriteria tersebut dihitung sebagai satu unit kerentanan dan kemudian dirangkum menjadi nilai V untuk masing-masing IKS.

C. Penentuan Kuantifikasi Nilai Ancaman (T)

Pada bagian ini, kami merumuskan nilai ancaman berdasarkan analisis terhadap kerentanan yang telah teridentifikasi pada setiap IKS. Nilai T ini bersifat potensial atau hipotetis, merepresentasikan kemungkinan skenario ancaman yang dapat terjadi jika kerentanan tersebut dieksploitasi oleh pihak tidak bertanggung jawab. Penilaian ini bertujuan untuk mengukur jumlah skenario ancaman yang mungkin timbul dari temuan kerentanan, sekaligus memahami pola serangan yang paling relevan terhadap *attack surface* yang dimiliki institusi.

Perhitungan nilai ancaman dilakukan secara kuantitatif dengan menghitung jumlah skenario ancaman yang dapat dirumuskan dari hasil eksplorasi OSINT. Penting untuk dicatat bahwa nilai ancaman (T) tidak selalu berbanding lurus dengan nilai kerentanan (V). Dalam praktiknya, satu atau lebih kerentanan yang berbeda dapat mengarah pada skenario ancaman yang sama (*many-to-one mapping*).

D. Pemetaan Skenario Ancaman

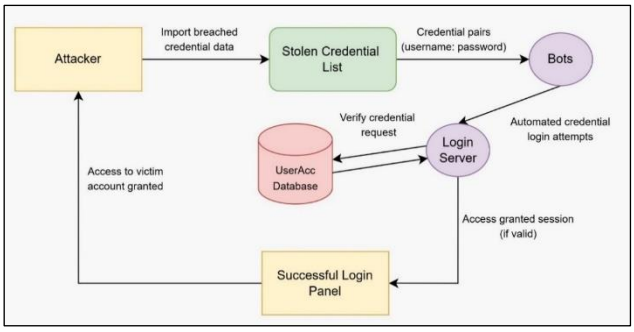
Pada bagian ini, skenario ancaman dalam penelitian dipetakan dengan terlebih dahulu memanfaatkan teknik *Open-Source Intelligence* (OSINT) guna mengidentifikasi potensi celah keamanan, permukaan serangan, layanan yang terbuka, dan informasi sensitif yang dapat disalahgunakan. Temuan OSINT ini menjadi landasan dalam merumuskan ancaman yang relevan dan realistis terhadap sistem yang diamati. Berdasarkan hasil klasifikasi nilai ancaman (*Low, Medium, High*), dipilih satu institusi IKS dari masing-masing kategori sebagai representasi untuk dijadikan sampel skenario.

Pemodelan skenario dilakukan karena terdapat keterkaitan langsung antara hasil observasi OSINT, kerentanan yang ditemukan, dan potensi ancaman yang mungkin muncul. Setiap skenario dirancang untuk menggambarkan kemungkinan eksploitasi berdasarkan hubungan logis antara temuan teknis dan ancaman. Sebagai contoh, salah satu skenario yang dikembangkan adalah serangan *credential stuffing*.

Untuk memvisualisasikan skenario, digunakan dua pendekatan utama:

a. *Data Flow Diagram* (DFD)

Untuk menggambarkan alur serangan credential stuffing secara menyeluruh, kami menggunakan *Data Flow Diagram* (DFD). *Credential stuffing* sendiri merupakan bentuk serangan otomatis yang memanfaatkan kredensial curian, hasil dari kebocoran data atau teknik perolehan ilegal lainnya, untuk diuji secara masif pada berbagai sistem dengan mekanisme autentikasi serupa. DFD yang disusun merepresentasikan proses otomatisasi *login* ini, menunjukkan interaksi antar entitas seperti *attacker*, bot otomatis, dan *login server*. Diagram ini secara visual memetakan bagaimana data kredensial mengalir dari sumber yang telah bocor hingga akhirnya berhasil memberikan akses ilegal ke akun korban.

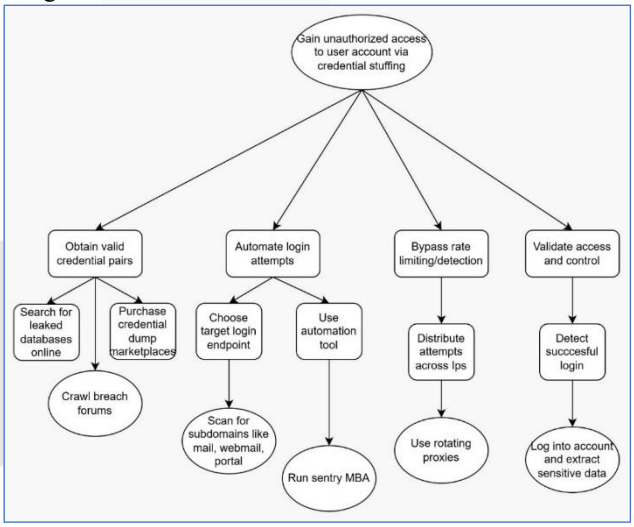


Gambar 3. *Data flow diagram brute-force login*

Berdasarkan DFD, serangan diawali saat penyerang memuat data kredensial hasil curian ke dalam daftar terstruktur, lalu menggunakan bot otomatis untuk mencoba *login* ke sistem target. Permintaan *login* dikirim ke server autentikasi untuk diverifikasi. Jika kredensial cocok, akses diberikan dan penyerang berhasil menguasai akun korban. Visualisasi ini menunjukkan bagaimana kredensial yang bocor dapat dimanfaatkan kembali dalam serangan otomatis, sekaligus menyoroti pentingnya perlindungan autentikasi dan deteksi terhadap aktivitas *login* mencurigakan.

b. *Attack Tree*

Untuk memperjelas proses serangan pada skenario *brute-force login*, dilakukan visualisasi dalam bentuk *attack tree*. Model ini digunakan untuk menggambarkan secara sistematis tahapan yang dilakukan oleh pelaku dalam upaya mendapatkan akses tidak sah ke akun pengguna, dengan cara menyalahgunakan kredensial yang telah bocor. Visualisasi ini membantu mengidentifikasi titik-titik kritis dalam proses serangan yang dapat dijadikan fokus utama dalam strategi mitigasi.



Gambar 4. *Attack tree brute-force login*

Berdasarkan *attack tree* di atas, serangan dimulai dari pencarian atau pembelian kredensial valid melalui forum pelanggaran data maupun *dump* pasar gelap. Kredensial ini kemudian digunakan dalam serangan otomatis terhadap *endpoint login* yang dipindai sebelumnya, seperti portal email atau sub*domain* internal lainnya. Untuk menghindari deteksi sistem keamanan, pelaku menyebarkan upaya *login* ke berbagai alamat IP menggunakan *rotating proxies*. Jika *login* berhasil, pelaku kemudian memperoleh akses penuh terhadap akun dan berpotensi mengekstrak data sensitif.

Ilustrasi ini menegaskan pentingnya perlindungan autentikasi seperti 2FA, pembatasan percobaan *login*, serta pemantauan aktivitas mencurigakan sebagai langkah pencegahan.

E. Klasifikasi Estimasi Nilai Risiko

Tahap ini melanjutkan pemetaan risiko kuantitatif terhadap delapan IKS dengan melakukan klasterisasi guna mengelompokkan institusi ke dalam kategori risiko secara sistematis. Meskipun bersumber dari data numerik, pendekatan ini bersifat kualitatif karena menekankan interpretasi distribusi nilai risiko. Metode yang digunakan adalah *equal interval classification*, yaitu membagi rentang nilai risiko (48–210) ke dalam tiga kelas dengan interval yang sama (sekitar 54), sehingga dihasilkan kategori Risiko Rendah (48–101), Risiko Sedang (102–155), dan Risiko Tinggi (156–210). Pendekatan ini dipilih untuk memastikan klasifikasi risiko yang objektif dan dapat dipertanggungjawabkan secara metodologis berdasarkan formula:

$$R = V \times T \times A$$

Dengan:

V = *Vulnerability*, yaitu tingkat keparahan kerentanan yang ditemukan melalui eksplorasi OSINT

T = *Threat*, yaitu tingkat potensi serangan hipotetis yang mungkin terjadi terhadap kerentanan yang ditemukan. Nilai T dihitung sebagai turunan dari V dengan mempertimbangkan dampak dan kemungkinan eksploitasi.

A = *Asset Value*, yang dalam penelitian ini direpresentasikan berdasarkan total nilai aset organisasi sebagaimana tercantum dalam data sekunder Publikasi Nasional

Dari hasil perhitungan di atas maka diperoleh lah hasil nilai estimasi risiko sebagai berikut:

Tabel 2. Perhitungan estimasi nilai risiko

No.	Nama IKS	Skor A	Skor V	Skor T	Nilai Risiko (R)
1.	Institusi Keuangan Syariah A	5	4	5	100
2.	Institusi Keuangan Syariah B	5	6	7	210
3.	Institusi Keuangan Syariah C	3	6	6	108
4.	Institusi Keuangan Syariah D	3	5	5	75
5.	Institusi Keuangan Syariah E	3	4	4	48
6.	Institusi Keuangan Syariah F	2	7	8	112
7.	Institusi Keuangan Syariah G	2	5	6	60
8.	Institusi Keuangan Syariah H	2	4	6	48

Berdasarkan hasil perhitungan di atas, setiap bank kemudian diklasifikasikan ke dalam kategori risiko yang telah ditetapkan sebelumnya. Adapun rinciannya disajikan dalam tabel berikut:

Tabel 3. Klasifikasi kategori nilai risiko

No.	Nama IKS	Nilai Risiko (R)	Kategori Risiko
1.	Institusi Keuangan Syariah A	100	Risiko Sedang
2.	Institusi Keuangan Syariah B	210	Risiko Tinggi
3.	Institusi Keuangan Syariah C	108	Risiko Sedang
4.	Institusi Keuangan Syariah D	75	Risiko Rendah
5.	Institusi Keuangan Syariah E	48	Risiko Rendah
6.	Institusi Keuangan Syariah F	112	Risiko Sedang
7.	Institusi Keuangan Syariah G	60	Risiko Rendah
8.	Institusi Keuangan Syariah H	48	Risiko Rendah

Dari hasil klasifikasi yang ditampilkan pada tabel, terlihat bahwa delapan IKS terbagi dalam tiga kategori risiko. Empat IKS diantaranya masuk kategori rendah (≤ 101), tiga IKS tergolong sedang (102–155), dan satunya berada di kategori tinggi (> 155). Variasi ini mencerminkan perbedaan signifikan dalam nilai aset, tingkat kerentanan, dan potensi ancaman di masing-masing institusi. Pengelompokan ini membantu memberikan gambaran awal yang lebih terfokus mengenai karakteristik risiko tiap entitas, sekaligus menjadi dasar untuk analisis lanjutan.

V. PENUTUP

A. Kesimpulan

Penelitian ini secara efektif memetakan potensi kerentanan dan ancaman siber pada layanan IT Institusi Keuangan Syariah melalui pemanfaatan berbagai *Open-Source Intelligence* (OSINT) *tools*. Eksplorasi ini mengungkapkan berbagai eksposur digital, mulai dari sub*domain* sensitif, kelemahan konfigurasi, hingga akses layanan penting, serta mengidentifikasi ancaman yang ditemukan merata di seluruh kategori aset IKS, Untuk mengkuantifikasi risiko, digunakan model $R=V\times T\times A$, di mana nilai aset (V) ditentukan dari temuan teknis, (T) adalah turunan dari tingkat kerentanan tersebut, dan (A) merefleksikan skala institusi, memungkinkan estimasi risiko yang objektif. Hasil pengukuran secara signifikan menunjukkan bahwa besarnya nilai aset tidak selalu berbanding lurus dengan tingkat risiko yang dihadapi. IKS dengan aset menengah dapat mencatatkan risiko tertinggi akibat eksposur digital yang tinggi, sementara IKS beraset lebih besar justru menunjukkan risiko rendah. Hal ini menegaskan bahwa penilaian ancaman siber harus melampaui indikator finansial dan secara kritis mempertimbangkan dimensi teknis eksposur digital yang diidentifikasi melalui OSINT, menekankan pentingnya peningkatan kesadaran dan upaya perlindungan keamanan digital yang proporsional dengan skala aset yang dikelola.

B. Saran

Berdasarkan hasil penelitian, disarankan untuk merancang strategi mitigasi yang proporsional sesuai dengan kategori estimasi risiko, baik secara teknis maupun non-teknis, dengan mempertimbangkan profil spesifik setiap institusi. Peningkatan kesadaran dan kewaspadaan terhadap eksposur layanan IT yang bersifat publik, seperti *website*, *subdomain*, dan sistem *email*, juga krusial mengingat temuan OSINT menunjukkan kerentanan akibat informasi atau konfigurasi sistem yang terbuka tanpa perlindungan memadai, yang berpotensi dieksploitasi. Untuk pengembangan selanjutnya, direkomendasikan agar metode penilaian risiko ditingkatkan dengan mempertimbangkan pembobotan tingkat keparahan (*severity weighting*) demi akurasi estimasi yang lebih tinggi, serta melakukan validasi lebih mendalam terhadap model skenario serangan yang saat ini bersifat konseptual. Selain itu, penelitian mendatang dapat berfokus pada penyusunan rancangan kebijakan, tata kelola, dan strategi mitigasi teknis yang aplikatif untuk mendukung pengendalian risiko secara komprehensif sesuai dengan profil ancaman yang teridentifikasi.

REFERENSI

[1] P. Nagendran, “Analysing and Reducing Vulnerability to OSINT ,” Universitetet I Oslo, 2024.

[2] Abdul Razzaq Matthew Aditya, Amelia Widya Octa Kuncoro Putri, Desta Lesmana Musthofa, and Pujo Widodo, “Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator),” *Global Political Studies Journal*, vol. 6, Apr. 2022.

[3] D. W. E. Simatangkir, E. F. N. Afifah, and N. S. Faliha, “KEAMANAN SIBER DALAM PERBANKAN SERTA TANTANGAN DAN SOLUSI DI ERA DIGITAL ,” *Jurnal Multidisiplin Ilmu Akademik* , vol. 2, Jan. 2025.

[4] IBM, “IBM X-Force 2025 Threat Intelligence Index,” 2025.

[5] BSSN, “LANSKAP KEAMANAN SIBER INDONESIA 2024,” Indonesia, 2024.

[6] Cameron Hashemi-Pour, “Definition public data,” TechTarget.

[7] D. Landoll, *The Security Risk Assessment Handbook*. Boca Raton: CRC Press, 2021. doi: 10.1201/9781003090441.

[8] I. Böhm and S. Lolagar, “Open source intelligence,” *International Cybersecurity Law Review*, vol. 2, no. 2, pp. 317–337, Dec. 2021, doi: 10.1365/s43439-021-00042-7.

[9] K. Christos, “Information Gathering Software,” European University Cyprus, 2023.

[10] A. Kipane, “Meaning of profiling of cybercriminals in the security context,” *SHS Web of Conferences*, vol. 68, p. 01009, Nov. 2019, doi: 10.1051/shsconf/20196801009.

[11] A. C. Laksono, “Threat Modeling pada Sistem Informasi Akademik Menggunakan Pendekatan STRIDE dan DREAD,” Universitas Islam Indonesia, 2020.

[12] K. K. Wicaksono and A. Fatulloh, “Aplikasi Manajemen Aset TI Berbasis Web (Studi Kasus PT. XYZ),” *G-Tech: Jurnal Teknologi Terapan*, vol. 6, no. 2, pp. 350–359, Oct. 2022, doi: 10.33379/gtech.v1i1.1736.

[13] N. A. Agustin and R. Meilani, “Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital,” Apr. 2024.