BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era transformasi digital saat ini, media sosial telah berevolusi dari sekadar platform interaksi menjadi pusat data yang krusial sekaligus vektor serangan siber yang sangat menarik bagi para aktor jahat. Fenomena ini diperparah dengan meningkatnya ketergantungan masyarakat pada platform seperti Facebook untuk berbagai aktivitas ekonomi dan sosial. Namun, seiring dengan itu, serangan rekayasa sosial (*social engineering*) terus berkembang dengan teknik yang semakin manipulatif[1].

Berdasarkan laporan monitoring keamanan siber terbaru, platform media sosial menjadi target utama karena besarnya volume informasi pribadi yang tersedia secara terbuka, yang memungkinkan penyerang melakukan serangan yang sangat personal dan meyakinkan. *Phishing* merupakan salah satu ancaman paling dominan di Indonesia[5]. Data dari *Indonesia Anti-Phishing Data Exchange* (IDADX) menunjukkan tren peningkatan penggunaan domain tingkat atas yang menyesatkan serta pemanfaatan layanan pihak ketiga untuk menyembunyikan identitas asli situs berbahaya tersebut.

Teknik yang digunakan tidak lagi sekadar mengirimkan pesan acak, melainkan menggunakan pola perilaku yang canggih untuk mengelabui filter keamanan platform media sosial. Keberhasilan serangan ini sangat bergantung pada ketidakwaspadaan pengguna terhadap ciri-ciri tautan berbahaya, terutama yang disebarkan melalui akun-akun yang terlihat sah atau memiliki aktivitas profil yang tampak norma[3]. Metode deteksi konvensional yang bersifat reaktif seringkali gagal mengantisipasi serangan sebelum korban jatuh.

Oleh karena itu, diperlukan pendekatan proaktif menggunakan *Open Source Intelligence* (OSINT). OSINT memungkinkan analis untuk mengumpulkan dan menghubungkan titik-titik data digital yang tersebar di sumber terbuka guna mengidentifikasi pelaku di balik kampanye *phishing* tersebut. Pemanfaatan data dari kebocoran data (*data breach*) yang diintegrasikan dengan alat investigasi modern menjadi tambang emas yang belum sepenuhnya dieksploitasi untuk tujuan pertahanan siber.

Berdasarkan observasi peneliti pada platform Facebook, banyak ditemukan akun-akun yang menyebarkan tautan berbahaya dengan kedok bantuan sosial, promo, atau konten provokatif lainnya. Investigasi awal menunjukkan bahwa jejak digital para pelaku ini sebenarnya tersimpan dalam database publik yang dapat diakses melalui teknik OSINT tertentu. Integrasi antara alat pemindaian URL proaktif dan pencarian identitas digital menjadi kunci dalam menekan angka keberhasilan serangan *phishing* di masa depan. Dengan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis pemanfaatan teknik OSINT dalam mengidentifikasi secara detail identitas pelaku penyebaran *phishing* guna memberikan langkah mitigasi yang lebih konkret bagi masyarakat dan praktisi keamanan siber[12].

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka permasalahan yang akan dibahas dalam penelitian ini dapat dirumuskan dalam bentuk pertanyaan sebagai berikut:

1. Bagaimana tahapan penerapan *Open Source Intelligence* (OSINT) untuk mengidentifikasi indikator-indikator awal potensi serangan *phishing* pada platform media sosial?
2. Apa saja karakteristik spesifik dari tautan, dan domain yang dapat diidentifikasi melalui OSINT sebagai penanda adanya kampanye serangan *phishing*?
3. Sejauh mana efektivitas OSINT dapat berkontribusi dalam membentuk strategi keamanan siber yang bersifat proaktif untuk deteksi dini (*early detection*) serangan *phishing*?

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan fokus pada tujuan utamanya, peneliti menetapkan beberapa batasan masalah. Batasan ini dibuat untuk memperjelas ruang lingkup penelitian dan variabel yang dianalisis. Adapun batasan-batasan tersebut adalah sebagai berikut:

1. Platform Media Sosial: Penelitian ini difokuskan pada analisis potensi serangan *phishing* yang terjadi secara spesifik pada platform media sosial Facebook..

2. Perangkat (Tools) yang Digunakan: Proses pengumpulan dan analisis data hanya akan menggunakan perangkat lunak *Open Source Intelligence* (OSINT).

3. Lingkup Identifikasi: Proses identifikasi pelaku dilakukan hingga tahap penemuan indikasi identitas (Nama, Lokasi, dan Data Demografis) berdasarkan korelasi data publik dan data bocor, tanpa melakukan peretasan (*hacking*) atau intrusi ilegal ke dalam sistem pribadi target.

1.4 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah untuk menganalisis secara mendalam efektivitas penggunaan teknik *Open Source Intelligence* (OSINT) dalam mendeteksi dan mengidentifikasi ancaman *phishing* yang tersebar di platform Facebook. Secara lebih terperinci, penelitian ini bertujuan untuk menguraikan tahapan sistematis dalam pengumpulan data intelijen sumber terbuka, mulai dari fase observasi postingan hingga fase ekstraksi metadata tautan berbahaya menggunakan perangkat seperti VirusTotal dan *Instant Data Scraper*.

Selain itu, penelitian ini bertujuan untuk mengklasifikasikan karakteristik teknis dari berbagai jenis domain *phishing* yang ditemukan, guna memahami pola rekayasa sosial yang paling sering digunakan oleh pelaku untuk mengelabui pengguna. Peneliti juga berupaya untuk memvalidasi akurasi data yang dihasilkan oleh perangkat bantu seperti bot Telegram investigasi dalam mengungkap identitas digital (*Personally Identifiable Information*) pelaku, termasuk e-mail, NIK, dan lokasi fisik, sebagai bagian dari proses atribusi ancaman.

Akhirnya, penelitian ini bertujuan untuk mengevaluasi kegunaan metode OSINT sebagai instrumen deteksi dini (*early detection*) yang dapat diintegrasikan ke dalam strategi pertahanan siber organisasi maupun individu. Dengan tercapainya tujuan-tujuan tersebut, penelitian ini diharapkan dapat memberikan kerangka kerja (*framework*) yang valid bagi praktisi keamanan siber dalam melakukan investigasi proaktif terhadap kejahatan siber di media sosial, serta memberikan dasar yang kuat dalam merumuskan langkah-langkah mitigasi yang lebih efektif.

1.5 Manfaat Penelitian

Penelitian mengenai pemanfaatan OSINT untuk identifikasi serangan *phishing* di Facebook diharapkan dapat memberikan manfaat yang signifikan, baik dari segi teoritis maupun praktis. Manfaat tersebut dijabarkan sebagai berikut:

1. Pengembangan Ilmu Keamanan Siber: Hasil penelitian ini diharapkan dapat memperkaya khazanah keilmuan di bidang keamanan siber, khususnya mengenai penerapan *Open Source Intelligence* (OSINT) sebagai metode proaktif dalam deteksi ancaman di platform media sosial.
2. Dasar Pengembangan Model Deteksi: Penelitian ini dapat menjadi landasan konseptual untuk pengembangan model atau kerangka kerja (*framework*) dalam mengidentifikasi dan mengklasifikasikan indikator-indikator serangan *phishing* yang lebih sistematis dan terstruktur.
3. Referensi Penelitian Mendatang: Menjadi acuan bagi peneliti selanjutnya yang ingin mengembangkan sistem otomasi deteksi *phishing* menggunakan *machine learning* yang berbasis pada fitur-fitur OSINT yang telah diidentifikasi dalam penelitian ini.

1.6 Sistematika Penulisan

BAB I: PENDAHULUAN Bab ini merupakan fondasi dasar penelitian yang menguraikan Latar Belakang Masalah mengenai urgensi ancaman *phishing* di Facebook dan potensi OSINT. Selanjutnya dipaparkan Rumusan Masalah, Batasan Masalah untuk menjaga fokus penelitian, Tujuan Penelitian yang ingin dicapai, serta Manfaat Penelitian baik secara akademis maupun praktis bagi masyarakat dan instansi keamanan siber.

BAB II: STUDI LITERATUR Bab ini berisi tinjauan pustaka yang merujuk pada penelitian-penelitian terdahulu (rentang 2020-2026) mengenai keamanan siber dan OSINT. Selain itu, bab ini menjabarkan Landasan Teori yang mencakup konsep rekayasa sosial, mekanisme *phishing*, serta cara kerja teknis dari perangkat investigasi yang digunakan seperti VirusTotal, *Instant Data Scraper*, Maltego, dan Bot Telegram investigatif. Bab ini diakhiri dengan Tabel Keaslian Penelitian untuk menunjukkan kebaruan (*novelty*) dari penelitian ini.

BAB III: METODOLOGI PENELITIAN Bab ini menjelaskan prosedur dan langkah-langkah sistematis dalam pelaksanaan penelitian. Pembahasan meliputi alur penelitian (*flowchart*), teknik pengumpulan data primer melalui observasi media sosial, serta tahapan analisis data menggunakan metode *atribusi siber*. Dijelaskan pula kriteria pemilihan target dan parameter validasi identitas yang digunakan selama proses investigasi.

BAB IV: HASIL DAN PEMBAHASAN Bab ini merupakan inti dari penelitian yang menyajikan hasil investigasi terhadap lima target akun penyebar *phishing* di Facebook. Pembahasan mencakup bukti-bukti teknis mulai dari temuan tautan berbahaya, hasil pemindaian reputasi domain, hingga pengungkapan identitas fisik pelaku (NIK, Alamat, dan Data Kendaraan) menggunakan bot OSINT. Bab ini juga menganalisis korelasi antar data digital yang ditemukan untuk membuktikan efektivitas metode yang diusulkan.

BAB V: KESIMPULAN DAN SARAN Bab terakhir ini berisi kesimpulan yang ditarik dari hasil analisis untuk menjawab rumusan masalah yang telah ditetapkan. Selain itu, bab ini memuat saran-saran strategis untuk pengembangan penelitian selanjutnya, serta rekomendasi bagi pihak terkait guna meningkatkan pertahanan terhadap serangan *phishing* di masa depan.