BAB I PENDAHULUAN

I.1 Latar Belakang

Internet telah mengalami perkembangan yang sangat pesat dengan memberikan kemudahan dalam pencarian data dan informasi publik melalui penerapan *Open-Source Intelligence* atau OSINT. OSINT adalah metode untuk memperoleh dan memanfaatkan informasi dari sumber-sumber terbuka dan tersedia secara publik. Namun demikian, peningkatan akses ke data publik dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan kejahatan. Risiko ini sejalan dengan meningkatnya kejahatan dunia maya.

Kejahatan dunia maya atau *cybercrime* merujuk pada aktivitas kriminal yang memanfaatkan jaringan komputer dan teknologi digital (Hidayah, 2020). *Cybercrime* tidak hanya menyerang sistem keamanan teknologi, tetapi juga dapat menyerang pengguna melalui serangan *social engineering*. *Social engineering* adalah bentuk serangan yang memanipulasi dan memanfaatkan kesadaran dan kesalahan manusia untuk mendapatkan informasi, salah satunya dengan *phishing* agar korban memberikan informasi pribadi secara tidak langsung melalui ancaman atau jebakan. Menurut Indonesia Anti-Phishing Data Exchange atau IDADX (2023), sebagaimana dikutip dalam "Laporan Aktivitas *Phishing Domain* ~.ID" periode Q1 2023, jumlah laporan *phishing* yang diterima mengalami kenaikan yang signifikan. Pada kuartal pertama tahun 2023, terdapat 26.675 laporan *phishing* dibandingkan dengan 6.106 laporan pada kuartal keempat tahun 2022, yang berarti terjadi peningkatan sebanyak 20.569 laporan *phishing*.

Di Indonesia, pernah terjadi kasus kebocoran data lebih dari 80% penduduk karena serangan siber, diantaranya *phishing*. Bagi organisasi yang menyimpan banyak data pribadi pegawai serta aset perusahaan, serangan *phishing* menyebabkan kerugian seperti kebocoran data dan informasi penting seperti akun pribadi berupa *email* atau *username* dan *password*, penurunan kepercayaan, dan kerusakan reputasi organisasi. Salah satu jenis serangan *phishing* yang menargetkan individu dengan jabatan tinggi pada sebuah organisasi atau perusahaan adalah *whaling attack*. *Whaling attack* dirancang menyerupai *email* bisnis penting yang tampak berasal dari otoritas yang sah dengan serangan *email*

spoofing. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis proses yang dilakukan sebelum melancarkan serangan *phishing* dengan jenis *whaling attack* dari berbagai kombinasi serangan. *Whaling attack* mencakup penggunaan *tools* dan serangan OSINT yang mewakili pencarian dan pengumpulan data publik, penggunaan *tools* dan serangan *social engineering* untuk membuat *cloned website* dan *phishing* URL, serta penggunaan *tool* dan serangan *email spoofing* dalam memalsukan dan mengirimkan *email* sehingga *email* tersebut seolah-olah berasal dari sumber yang sah. Namun, *whaling attack* yang dilakukan tidak sampai ke tahap *attack launching* atau eksploitasi. Dari perumusan *whaling attack* tersebut, penyerang dapat memperoleh data kredensial taget. Penelitian ini akan mengolah hasil *whaling attack* dari penyusunan DFD atau *data flow diagram* serangan menjadi sebuah kerangka penyerangan yang disebut dengan *attack tree*. *Attack tree* merupakan metode yang digunakan untuk menggambarkan keamanan suatu sistem dengan mengidentifikasi berbagai kemungkinan jenis serangan. *Attack tree* memungkinkan analisis lebih mendalam untuk mengembangkan strategi penyerangan. Pada analisis, akan dilakukan perbandingan hasil serangan *whaling attack* berdasarkan metrik yang diukur dalam proses perumusan serangan OSINT, *social engineering*, dan *email spoofing*. Hasil analisis bertujuan untuk mengetahui dan memahami karakteristik *whaling attack* berdasarkan metrik tertentu menggunakan *attack tree*.

I.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan untuk penelitian ini adalah:

a. Bagaimana cara merumuskan *whaling attack* menggunakan *threat modelling* berdasarkan serangan OSINT, *social engineering*, dan *email spoofing*?
b. Bagaimana cara mengenali salah satu karakteristik dari *attack tree*?
c. Bagaimana cara membedakan satu *attack tree* dengan *attack tree* lain yang dirumuskan dari setiap kombinasi *whaling attack*?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Merumuskan *whaling attack* dari berbagai macam serangan yang berbeda.
b. Merumuskan karakteristik *attack tree* berdasarkan metrik dari elemen masing-masing serangan.
c. Merumuskan metrik *time* untuk mengenali, membedakan, dan mengkategorikan *attack tree*.

I.4 Batasan Penelitian

Adapun batasan penelitian adalah:

a. Perumusan dan pemodelan *whaling attack* tidak dilakukan hingga tahap *attack launching* (eksploitasi).
b. Penelitian ini tidak membahas aspek kerentanan dan mitigasi dari target serangan.
c. Analisis metrik *time* dari *whaling attack* menggunakan kategori *real time*.

I.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Secara teoritis
    a. Menambah wawasan mengenai serangan *social engineering* yang menargetkan kesadaran manusia.
    b. Memahami relasi antara data yang sifatnya publik yang dapat digunakan untuk melakukan serangan *social engineering* berupa *whaling attack.*
2. Secara Praktis
    a. Mengetahui fungsi praktis dari OSINT, *social engineering*, dan *email spoofing tools*.
    b. Menambah pengetahuan praktis mengenai cara kerja dan mekanisme *whaling attack*.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi uraian perumusan masalah terkait bagaimana cara merumuskan *whaling attack* menggunakan *threat modelling*, mengenali karakteristik *attack tree,* dan membedakan *attack tree* satu dengan *attack tree* lain berdasarkan eksperimen serangan OSINT, *social engineering,* dan *email spoofing*. Tujuan penelitian ini adalah merumuskan *whaling attack* dari berbagai macam serangan, merumuskan *attack tree* berdasarkan metrik, serta mengenali, membedakan, dan mengkategorikan *attack tree* berdasarkan karakteristik metrik *time*. Batasan penelitian ini adalah perumusan dan pemodelan *whaling attack* tidak dilakukan sampai tahap eksploitasi, tidak membahas aspek kerentanan dan mitigasi dari serangan yang dilakukan, serta analisis metrik *time* hanya diukur berdasarkan kategori *real time*. Penelitian ini memiliki manfaat secara teoritis yang akan menambah wawasan mengenai serangan *social engineering* yang memanfaatkan kesadaran manusia, serta memahami relasi antara data publik yang dapat digunakan untuk melakukan *whaling attack*. Secara praktis, penelitian ini akan menjelaskan fungsi praktis dari OSINT, *social engineering,* dan *email spoofing* serta mengetahui cara kerja dan mekanisme *whaling attack*.

BAB II TINJAUAN PUSTAKA

Bab ini berisi literatur atau teori yang relevan dengan permasalahan yang sedang diteliti, seperti data publik, *open-source intelligence*, *social engineering*, *email spoofing*, *phishing*, *whaling attack*, *flowchart diagram*, *data flow diagram*, *threat modelling*, *attack tree* dan metrik *time* yang akan menjadi dasar pengetahuan umum untuk mendukung topik penelitian mengenai pemodelan *whaling attack*.

BAB III METODOLOGI PENELITIAN

Bab ini berisi metode konseptual yang terdiri dari *Environment*, IS *Research,* dan *Knowledge Base*. Bagian *Environment* berisi aspek *people*, *organization,* dan *technology*. Bagian IS *Research* berisi *develop*/*build* dan *justify*/*evaluate*. Bagian *Knowledge Base* berisi *foundations* dan *methodologies*. Bab ini juga berisi sistematika penyelesaian masalah yang dibuat dalam enam tahap, yaitu tahap awal, tahap hipotesis, tahap desain, tahap eksperimen, tahap analisis, dan tahap akhir.

BAB IV PERANCANGAN DAN ALUR EKSPERIMEN

Bab ini berisi tahapan eksperimen yang dimulai dari perencanaan dan persiapan eksperimen berupa spesifikasi perangkat keras dan perangkat lunak yang digunakan, daftar IP *address,* platform eksperimen, alur eksperimen, implementasi eksperimen, dan data hasil eksperimen dari serangan OSINT, *social engineering*, dan *email spoofing*.

BAB V ANALISIS

Bab ini berisi analisis perumusan serangan OSINT, *social engineering*, dan *email spoofing*, analisis data serangan, perumusan kombinasi serangan yang menghasilkan *whaling attack*, perumusan *attack tree*, serta pengkategorian *whaling attack* berdasarkan metrik *time*. Pada bab ini dipaparkan juga hasil analisis berupa perbandingan setiap *whaling attack* berdaasarkan metrik *time*.

BAB VI KESIMPULAN DAN SARAN

Bab ini memaparkan kesimpulan dari seluruh kegiatan penelitian yang dilakukan. Pada bab ini dipaparkan juga saran yang dapat digunakan sebagai pertimbangan untuk penelitian selanjutnya.