BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi sistem informasi yang semakin maju memberikan kemudahan suatu organisasi ataupun individu untuk menyimpan, mengolah, dan menyebarkan data ke publik. Namun, teknologi sistem informasi yang semakin maju memiliki risiko kebocoran data yang tinggi jika tidak dikelola dengan baik. Salah satu faktor kebocoran data adalah *spear phishing attack*. *Spear phishing attack* merupakan salah satu jenis *phishing attack* yang menargetkan serangan pada suatu individu yang lebih spesifik dengan mengirimkan *email* untuk mendapatkan data kredensial target (Yuliadarnita et al., 2023). *Phishing attack* berdasarkan pada laporan *Cost of a Data Breach Report* 2021 disusun oleh *International Business Machines* (IBM) merupakan salah satu dari sepuluh *attack vectors* yang menempati posisi ke dua sebesar 17% yang masih digunakan penyerang untuk mencuri data (Arizal et al., 2023).

Kondisi ini perlu menjadi perhatian pada instansi XYZ dikarenakan Indonesia pernah mengalami kebocoran data dengan kerugian mencapai sekitar 600 triliun rupiah dimana terdapat 80% data warga Indonesia didalamnya yang tersebar pada aplikasi dan *website* yang pastinya menyimpan banyak data pribadi seperti informasi pegawai, informasi aset terenkripsi, dan informasi identitas pengguna (Setiawan et al., 2022). Data pribadi yang merupakan aset yang harus dilindungi oleh suatu organisasi maupun individu, informasi data pribadi bersifat privasi dan harus dilindungi dengan tujuan agar tidak disalahgunakan oleh pihak yang tidak berkepentingan yang dapat menyebabkan kerugian bagi organisasi maupun individu (Ansyafa et al., 2024). Oleh karena itu, diperlukan adanya pengujian keamanan terhadap perlindungan data di instansi XYZ. Penelitian ini akan melakukan percobaan pengujian dengan salah satu jenis *phishing attack* yaitu *spear phishing attack* dengan memanfaatkan data publik sebagai target. Dengan menggunakan metode *Open Source Intelligence* (OSINT) *tools* untuk mengetahui kerentanan dengan mendapatkan data secara publik. Selain itu, memanfaatkan serangan *social engineering tools* untuk memanipulasi psikologis target untuk mengirimkan *email spoofing*. Dalam percobaan penyerangan akan diolah dan

dianalisis untuk dilakukan pengukuran dari kumpulan informasi data pribadi yang didapatkan berdasarkan metrik pada *attack tree diagram* dari *threat modeling spear phishing attack*. Analisis dilakukan dengan membandingkan dari data hasil pengujian berdasarkan dengan metrik yang diukur pada proses *spear phishing attack*. Hasil analisis yang didapat bertujuan untuk mengetahui karakter pada *threat modeling* berdasarkan metrik yang digunakan pada *attack tree*.

I.2 Perumusan Masalah

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

1. Bagaimana cara menyusun *threat modeling* dari *spear phishing attack* dalam *attack tree* berdasarkan serangan OSINT, *social engineering*, dan *email spoofing*?
2. Bagaimana menyusun relasi dan mengidentifikasi karakter dari beberapa *attack tree*?
3. Bagaimana cara membandingkan *attack tree* berdasarkan metrik granularitas data?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Menganalisa dan menyusun *spear phishing attack* dari berbagai macam serangan.
b. Menyusun dan mengidentifikasi *attack tree* berdasarkan data, relasi antar *node*, dan karakteristik pada *attack tree* dari *data flow diagram*.
c. Menganalisa perbandingan penggunaan metrik granularitas data untuk mengetahui perbedaan rincian data yang didapatkan pada *attack tree*.

I.4 Batasan Penelitian

Adapun batasan penelitian pada penelitian ini sebagai berikut:

a. Penelitian ini berdasar pada eksperimen dan pemodelan *spear phishing attack* tidak sampai pada tahap eksploitasi.

b. Penelitian ini dibatasi pada analisa *attack tree* berkaitan dengan serangan *spear phishing attack*, sehingga tidak membahas aspek kerentanan dan mitigasi dari serangan.
c. Pembahasan perbandingan metrik granularitas data pada *attack tree* dari *spear phishing attack* menggunakan ketegori tingkat.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis
   a. Dapat menambah pengetahuan terkait dengan ancaman keamanan serangan OSINT, *social engineering*, dan *email spoofing* berdasarkan penyusunan *attack tree* dari *spear phishing attack.*
   b. Dapat mengenali karakter *attack tree* berdasarkan metrik granularitas data.
2. Secara praktis
   a. Dapat mengetahui dan mengenali ancaman keamanan *spear phishing attack* yang berlangsung dengan langkah-langkah pada proses serangan.
   b. Dapat memahami penggunaan berbagai *software opensource* dengan fungsi yang berbeda yaitu OSINT, *social engineering*, dan *email spoofing*.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini berisikan perumusan masalah terkait bagaimana cara menyusun *spear phishing attack* menggunakan *threat modeling*, mengidentifikasi karakter dari *attack tree*, dan membandingkan *attack tree* berdasarkan metrik granularitas data berdasarkan eksperimen serangan OSINT, *social engineering*, dan *email spoofing*. Bab ini juga menguraikan tujuan penelitian menyusun *spear phishing attack* dari berbagai serangan, mengidentifikasi *attack tree* berdasarkan data, relasi antar *node*, dan karakteristik pada *attack tree* dari *data flow diagram*, serta menganalisa perbandingan penggunaan

metrik granularitas data pada *attack tree*. Batasan penelitian ini yaitu terbatas pada eksperimen dan pemodelan *spear phishing attack*, analisa *attack tree* berkaitan dengan serangan *spear phishing attack* tidak membahas aspek kerentanan dan mitigasi serangan, serta perbandingan metrik granularitas berdasarkan *attack tree*. Penelitian ini juga memiliki manfaat secara teoritis dan secara praktis.

Bab II Tinjauan Pustaka

Bab ini berisi literatur terkait teori atau dasar ilmiah yang relevan dengan permasalahan pada penelitian seperti OSINT, data publik, ancaman (*threat*), keamanan siber (*cyber security*), *social engineering*, *phishing attack*, *spear phishing attack*, *email spoofing*, metrik granularitas data, *attack tree*, *Data Flow Diagram* (DFD), diagram alur (*flowchart*), telnet, *Simple Mail Transfer Protocol* (SMTP) dan Kali Linux. Bab ini juga menjelaskan temuan-temuan sebelumnya yang berkaitan dengan penelitian saat ini yang dapat membantu memperluas pemahaman terkait subjek yang sedang diteliti.

Bab III Metodologi Penelitian

Bab ini menjelaskan metode konseptual terdiri dari Lingkungan, Penelitian, dan Dasar Ilmu. Bagian Lingkungan berisikan aspek *people*, *oganizations*, dan *technology*. Bagian Penelitian berisikan *build* dan *evaluate*. Bagian dasar ilmu berisikan *foundations* dan methodologies. Bab ini juga yang berisikan sistematika penyelesaian masalah yang menguraikan enam tahap, yaitu tahap awal, tahap hipotesis, tahap desain, tahap eksperimen, tahap analisis, dan tahap akhir. Selain itu, bab ini berisikan penjelasan mengenai pengumpulan data, pengolahan data, sampai dengan tahap akhir metode evaluasi.

BAB IV Perencanaan dan Alur Eksperimen

Bab ini berisi uraian dari perencanaan dan persiapan untuk eksperimen berupa spesifikasi perangkat keras, perangkat lunak, *platform* eksperimen, dan IP *address* yang digunakan, serta alur

eksperimen, implementasi eksperimen, dan data hasil eksperimen dari serangan OSINT, *social engineering*, dan *email spoofing*.

Bab V Analisis

Bab ini berisi analisis dari hasil perumusan serangan OSINT, *social engineering*, dan *email spoofing*, analisis data serangan, perumusan kombinasi serangan yang menghasilkan *spear phishing attack*, perumusan *attack tree*, dan pengkategorian berdasarkan metrik granularitas data. Pada bab ini juga dipaparkan hasil analisis dari perbandingan kombinasi serangan *spear phishing attack* berdasarkan metrik granularitas, dan terdapat ringkasan analisis.

Bab VI Kesimpulan dan Saran

Bab ini berisi kesimpulan dari keseluruhan kegiatan yang telah dilakukan pada penelitian. Bab ini juga memaparkan saran yang dapat menjadi pertimbangan untuk penelitian selanjutnya.