Implementasi Dan Analisis *Attack Tree* Pada Serangan *Email Phishing* Dalam Skema *Business Email Compromise Attack* Di Instansi Xyz Dengan Metrik Kompleksitas

Amirrahma Hamida
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
amirahmahmd@student.telkomuniversity.ac.id

Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

Avon Budiono
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
avonbudi@telkomuniversity.ac.id

Abstrak* — Serangan *email phishing* dalam skema *Business Email Compromise* (BEC) merupakan ancaman siber yang mengeksploitasi komunikasi organisasi melalui kombinasi manipulasi psikologis dan teknik rekayasa teknis. Penelitian ini bertujuan untuk mengimplementasikan serta menganalisis skenario serangan *email phishing* pada Instansi XYZ menggunakan pendekatan *attack tree* dan metrik kompleksitas. Metodologi penelitian meliputi pengumpulan informasi melalui *Open-Source Intelligence* (OSINT) menggunakan Skrapp.io, Tomba.io, dan Phonebook.cz, simulasi *social engineering* menggunakan Socialphish, serta pengiriman *spoofed email* melalui protokol SMTP menggunakan Telnet. Data hasil eksperimen dimodelkan ke dalam *Data Flow Diagram* (DFD) untuk mengidentifikasi aliran data dan dependensi antar proses, kemudian ditransformasikan menjadi model *attack tree*. Setiap jalur serangan dievaluasi menggunakan parameter *Skill* (S), *Time* (T), dan *Cost* (R) untuk menghitung tingkat kompleksitasnya. Hasil analisis menunjukkan bahwa skenario yang menggunakan Tomba.io memiliki nilai kompleksitas terendah sebesar 30, diikuti Phonebook.cz sebesar 32 dan Skrapp.io sebesar 42. Dengan nilai kompleksitas tersebut, Tomba.io teridentifikasi sebagai *path of least resistance*, yaitu jalur serangan yang memerlukan hambatan paling rendah untuk mencapai tujuan serangan. Temuan ini menunjukkan bahwa efektivitas *tools* OSINT dalam memperoleh informasi target berpengaruh langsung terhadap tingkat kemudahan pelaksanaan serangan. Penelitian ini menyimpulkan bahwa rendahnya hambatan pada fase OSINT secara signifikan meningkatkan peluang keberhasilan skema BEC, sehingga organisasi perlu memperkuat keamanan email dan membatasi eksposur informasi publik untuk mengurangi risiko serangan.

Kata kunci: Attack tree, Metrik kompleksitas, Email phishing, OSINT

I. PENDAHULUAN

Transformasi digital meningkatkan risiko ancaman keamanan informasi, salah satunya serangan phishing email dalam skema *Business Email Compromise* (BEC). Serangan ini memanfaatkan rekayasa sosial untuk memperoleh informasi sensitif maupun kredensial korban melalui email palsu yang menyerupai komunikasi resmi organisasi. Berdasarkan laporan Verizon Data Breach Investigation Report 2025, sebagian besar serangan social engineering memanfaatkan email sebagai media utama. Instansi XYZ sebagai organisasi besar memiliki potensi kerentanan terhadap serangan BEC karena banyaknya informasi publik yang tersedia secara daring. Penelitian ini berfokus pada pemodelan serangan phishing email menggunakan *attack tree* untuk mengetahui jalur serangan dengan kompleksitas terendah berdasarkan parameter *Skill* (S), *Time* (T), dan *Cost* (R).

II. KAJIAN TEORI

A. *Open Source Intelligent (*OSINT)

OSINT merupakan metode pengumpulan informasi dari sumber terbuka seperti media sosial, website resmi, dan database publik yang tidak dilindungi oleh hukum dan bersifat legal. Pada penelitian ini digunakan Skrapp.io, Tomba.io, dan Phonebook.cz untuk memperoleh data email target.

B. *Attack Tree*

Attack Tree digunakan sebagai pendekatan untuk memetakan alur serangan secara bertingkat, dengan menjabarkan sasaran akhir yang ingin dicapai penyerang ke dalam sejumlah langkah dan tindakan teknis yang dilakukan pada tiap fase serangan. (Schneier, 1999).

- *Root Node*: Tujuan utama mendapatkan kredensial (Get Credentials Data).
- *Intermediate Nodes*: Sub-tujuan serangan (OSINT, Social Engineering, Spoofing).
- *Leaf Nodes:* Tindakan operasional spesifik yang dinilai menggunakan metrik keamanan (Wang & Wang, 2017).

C. Metrik Kompleksitas

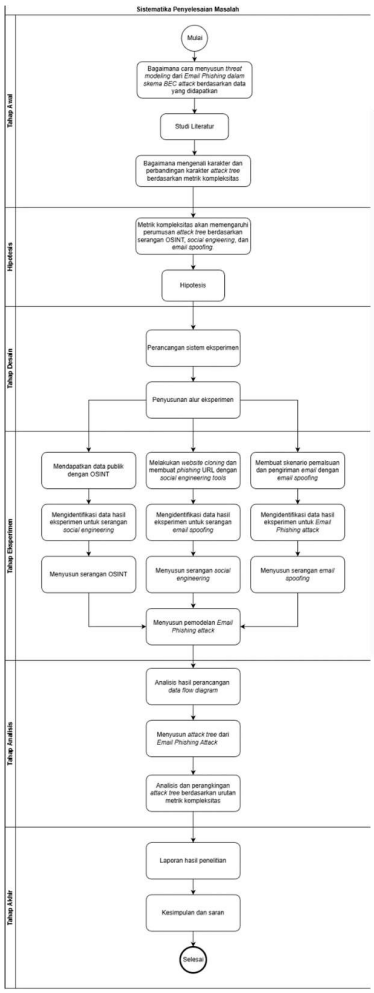
Pada penelitian ini, metrik kompleksitas diterapkan untuk mengukur tingkat kerumitan serangan berdasarkan parameter Skill, Time, dan Cost. Jalur dengan nilai kompleksitas paling rendah diidentifikasi sebagai jalur serangan yang paling efektif karena memerlukan sumber daya yang lebih sedikit dibandingkan alternatif lainnya. Metrik tersebut digunakan sebagai pendekatan kuantitatif untuk mengevaluasi tingkat kesulitan, kebutuhan sumber daya, serta probabilitas

keberhasilan serangan dengan merujuk pada konsep Attack Tree yang diperkenalkan oleh Schneier (1999).

III. METODE

A. Sistematika Penyelesaian Masalah

Penelitian ini diawali dengan identifikasi permasalahan terkait pemodelan serangan *email phishing* dalam skema BEC, yang kemudian diperkuat melalui studi literatur mengenai OSINT, *social engineering, email spoofing* dan pembentukan *attack tree* serta metrik kompleksitas. Berdasarkan hasil kajian tersebut, dirancang skenario eksperimen yang memanfaatkan beberapa *tools* OSINT untuk memperoleh informasi target, dilanjutkan dengan pembuatan skenario *social engineering* dan pengiriman *spoofed email* sebagai simulasi serangan BEC. Hasil pemetaan kemudian digunakan sebagai dasar penyusunan model *attack tree* yang merepresentasikan tahapan serangan secara hierarkis. Hasil perhitungan nantinya akan dibandingkan guna mengidentifikasi jalur serangan dengan tingkat kompleksitas terendah yang berpotensi menjadi *path of least resistance* pada Instansi XYZ. Berikut adalah alur lengkap dalam sistematika penyelesaian masalah.



GAMBAR 1
Sistematika Penyelesaian Masalah

B. Metrik Kompleksitas

Tahapan penelitian mencakup proses pengumpulan data melalui pemanfaatan OSINT, simulasi serangan *social engineering*, dan pengiriman email hasil *spoofing*. Seluruh data yang diperoleh dari rangkaian eksperimen kemudian dimodelkan menggunakan *Data Flow Diagram* (DFD) sebelum dikembangkan menjadi struktur *attack tree*. Selanjutnya, setiap *leaf node* pada *attack tree* dievaluasi menggunakan parameter *Skill* (S), *Time* (T), dan *Cost* (R) dengan skala penilaian 1–5. Akumulasi nilai dari ketiga parameter tersebut digunakan untuk menentukan jalur serangan dengan tingkat kompleksitas atau resistensi terendah. Berikut adalah kalkulasi dan propagasi nilai untuk memperhitungkan nilai dari *attack tree*:

- Rumus jalur untuk gerbang AND.

$$C\ path = \sum (\mathrm{S} + \mathrm{T} + \mathrm{R})$$

- Jika terdapat gerbang OR, maka jalur dengan nilai C terkecil yang akan diambil dalam analisis akhir, karena merepresentasikan jalur termudah bagi penyerang.

IV. HASIL DAN PEMBAHASAN

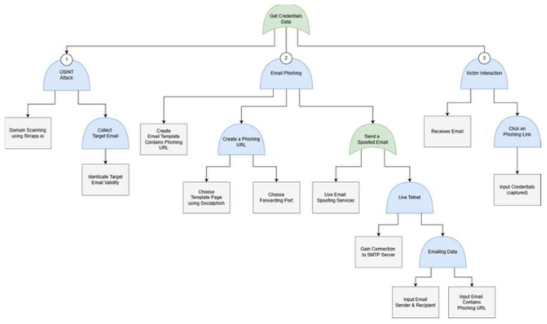
Hasil penelitian menunjukkan bahwa ketiga tools OSINT berhasil memperoleh data publik berupa alamat email dan pola komunikasi organisasi. Informasi tersebut kemudian digunakan dalam simulasi *phishing* menggunakan Socialphish dan pengiriman email palsu melalui telnet.

Model *attack tree* berhasil memetakan tahapan serangan mulai dari proses pengumpulan data, manipulasi psikologis, hingga pengiriman *email spoofing*. Berdasarkan hasil perhitungan metrik kompleksitas, diperoleh hasil sebagai berikut:

A. Attack Tree

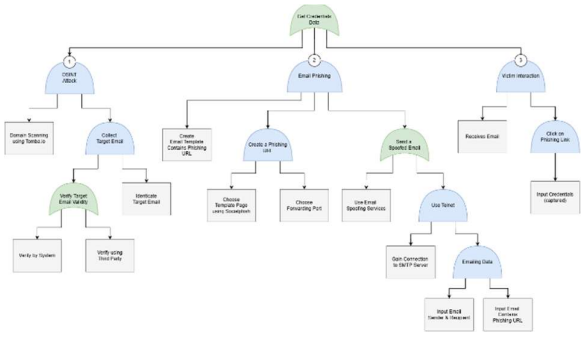
Berdasarkan hasil pemodelan proses serangan yang diperoleh dari DFD, dibangun struktur *attack tree* untuk merepresentasikan tahapan serangan *email phishing* dalam skema BEC secara hierarkis. Model ini menggambarkan hubungan antara tujuan utama serangan, sub-tujuan, serta aktivitas teknis yang dilakukan penyerang untuk mencapai keberhasilan serangan. Selain itu, *attack tree* digunakan sebagai dasar dalam analisis metrik kompleksitas melalui parameter *Skill* (S), *Time* (T), dan *Cost* (R), untuk mengidentifikasi jalur serangan yang paling efektif. Berikut adalah struktur *attack tree* berdasarkan OSINT *tools* yang digunakan.

- Skrapp.io



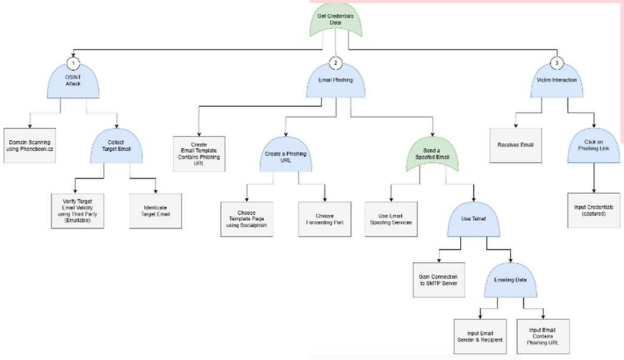
GAMBAR 2
Attack Tree Skrapp.io

- Tomba.io



GAMBAR 3
Attack Tree Tomba.io

- Phonebook.cz



GAMBAR 4
*Attack Tree*Phonebook.cz

B. Tabel Hasil Perhitungan

Temuan penelitian memperlihatkan bahwa penggunaan Tomba.io menghasilkan jalur serangan yang memerlukan sumber daya paling sedikit dibandingkan alternatif lainnya, sehingga dikategorikan sebagai *path of least resistance*. Kondisi tersebut mengindikasikan bahwa ketersediaan informasi publik organisasi dapat mempermudah proses pengumpulan intelijen oleh penyerang dan mendukung penyusunan skenario phishing yang lebih persuasif serta sulit dibedakan dari komunikasi yang sah.

TABEL 1
Tabel Hasil Perhitungan

OSINT Tools	Metrik Kompleksitas			
	Skill	Time	Cost	Total
Tomba.io	10	10	10	30
Phonebook.cz	11	10	11	32
Skrapp.io	15	14	13	42

C. Analisis Komparatif

Analisis komparatif menunjukkan bahwa ketiga skenario memiliki karakteristik yang serupa pada tahap eksekusi serangan dan struktur biaya karena menggunakan infrastruktur serta tools yang relatif sama. Hambatan utama serangan terletak pada proses koneksi SMTP yang membutuhkan kemampuan teknis lebih tinggi dibandingkan tahap lainnya.

Perbedaan nilai kompleksitas terutama dipengaruhi oleh efektivitas tools OSINT dalam memperoleh informasi target. Tomba.io menghasilkan nilai kompleksitas terendah sebesar 30 sehingga menjadi *path of least resistance*, diikuti Phonebook.cz dengan nilai 32. Sementara itu, Skrapp.io memperoleh nilai tertinggi sebesar 42 karena memerlukan lebih banyak proses validasi dan interaksi manual. Hasil ini menunjukkan bahwa efisiensi pengumpulan informasi pada tahap OSINT berpengaruh langsung terhadap tingkat kompleksitas keseluruhan serangan.

V. KESIMPULAN

Penelitian ini berhasil mengimplementasikan pemodelan serangan *email phishing* dalam skema BEC menggunakan pendekatan *attack tree* dan metrik kompleksitas. Hasil analisis menunjukkan bahwa pemanfaatan OSINT berperan dalam menurunkan hambatan serangan dengan mempermudah proses pengumpulan informasi target. Berdasarkan perhitungan metrik kompleksitas yang menggunakan parameter *Skill* (S), *Time* (T), dan *Cost* (R), skenario yang memanfaatkan Tomba.io memperoleh nilai kompleksitas terendah sebesar 30, diikuti oleh Phonebook.cz dengan nilai 32, dan Skrapp.io dengan nilai 42.

Perbedaan nilai tersebut menunjukkan bahwa kemampuan *tools* OSINT dalam menyediakan informasi target memengaruhi tingkat kemudahan pelaksanaan serangan. Tomba.io teridentifikasi sebagai *path of least resistance* karena menghasilkan jalur serangan yang paling efisien dibandingkan skenario lainnya. Temuan ini menegaskan bahwa informasi organisasi yang tersedia secara publik dapat dimanfaatkan untuk mendukung penyusunan skema *phishing* yang lebih meyakinkan. Oleh karena itu, organisasi perlu memperkuat keamanan email, meningkatkan kesadaran pengguna terhadap ancaman *phishing*, serta membatasi eksposur informasi publik guna meminimalkan risiko serangan BEC.

REFERENSI

- Books

[1] K. D. Mitnick and W. L. Simon. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2003.

- Journal Articles

[2] M. Glassman and M. J. Kang. “Intelligence in the Internet Age: The Emergence and Evolution of Open-Source Intelligence (OSINT).” Computers in Human Behavior, vol. 28, no. 2, pp. 673–682, 2012.
[3] I. R. A. Hamid and J. H. Abawajy. “An Approach for Profiling Phishing Activities.” Computers & Security, vol. 45, pp. 27–41, 2014.
[4] N. Saud Al-Musib, F. Mohammad Al-Serhani, M. Humayun, and N. Z. Jhanjhi. “Business Email Compromise (BEC) Attacks.” Materials Today: Proceedings, vol. 81, pp. 497–503, 2023.
[5] Z. Wang, H. Zhu, and L. Sun. “Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods.” IEEE Access, vol. 9, pp. 11895–11910, 2021.
[6] E. J. Williams and A. N. Joinson. “Developing a Measure of Information Seeking About Phishing.” Journal of Cybersecurity, vol. 6, no. 1, 2020.
[7] M. Lopuhaä-Zwakenberg, C. E. Budde, and M. Stoelinga. “Efficient and Generic Algorithms for Quantitative Attack Tree Analysis.” IEEE Transactions

on Dependable and Secure Computing, vol. 20, no. 5, pp. 4169–4187, 2023.
[8] E. Lakomaa and J. Kallberg. "Open Data as a Foundation for Innovation: The Enabling Effect of Free Public Sector Information for Entrepreneurs." IEEE Access, vol. 1, pp. 558–563, 2013.
[9] Z. Xiang, D. J. Miller, and G. Kesidis. "Reverse Engineering Imperceptible Backdoor Attacks on Deep Neural Networks for Detection and Training Set Cleansing." Computers & Security, vol. 106, 2021.
[10] Febriyani. "Security Awareness Strategy for Email Phishing Scams: A Case Study One of a Company in Singapore." Journal of Information and Visualization, vol. 7, no. 2, 2023.
[11] A. Sutanti, M. K. Mz, M. Mustika, and P. Damayanti. "Rancang Bangun Aplikasi Perpustakaan Keliling Menggunakan Pendekatan Terstruktur." Komputa: Jurnal Ilmiah Komputer dan Informatika, vol. 9, no. 1, pp. 1–8, 2020.
[12] M. Irfan, D. Mirwansyah, and K. Az Zahro. "Perancangan Sistem Informasi Monitoring Akademik Dengan Menggunakan Data Flow Diagram." Jurnal Locus Penelitian dan Pengabdian, vol. 2, no. 12, pp. 1201–1207, 2024.

- Conference Proceedings

[13] K. Kaushik, I. Punhani, S. Sharma, and M. Martolia. "An Advanced Approach for Performing Cyber Fraud Using Banner Grabbing." Proceedings of the 5th International Conference on Contemporary Computing and Informatics (IC3I), pp. 298–302, 2022.
[14] L. Metongnon and R. Sadre. "Beyond Telnet: Prevalence of IoT Protocols in Telescope and Honeypot Measurements." Proceedings of the Workshop on Traffic Measurements for Cybersecurity, pp. 21–26, 2018.

- Electronic / Online References

[15] H. Hu and G. Wang. "Revisiting Email Spoofing Attacks." [Online]. Available: https://doi.org/10.48550/arXiv.1801.00853
[16] A. Gioti. "Advancements in Open-Source Intelligence (OSINT) Techniques and the Role of Artificial Intelligence in Cyber Threat Intelligence (CTI)." [Online].
[17] M. Ahsan. Analisa Kerentanan Sistem Dengan Menerapkan Open Vulnerability Assessment System Menggunakan Greenbone Vulnerability Management (GVM). [Online]. Available: https://repository.mercubuana.ac.id/69181/

- Thesis / Academic Reports

[18] A. L. Suryana, R. E. Akbar, and N. Widiyasono. "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)." Jurnal Edukasi dan Penelitian Informatika, vol. 2, no. 2, 2016.