Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

Pemodelan Attack Tree Pada Spear Phishing Attack di Instansi Publik dengan Metrik Granularitas Data

Anisa Wahyu Pratiwi*, A Widjajarto, Avon Budiyono

Fakultas Rekayasa Industri, Program Studi Sistem Informasi, Universitas Telkom, Bandung
Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat, Indonesia
Email: [1,*]anisawahyup@student.telkomuniversity.ac.id, [2]adtwjrt@telkomuniversity.ac.id, [3]avonbudi@telkomuniveristy.ac.id
Email Penulis Korespondensi: anisawahyup@student.telkomuniversity.ac.id
Submitted: **02/09/2024;** Accepted: **09/10/2024;** Published: **06/04/2025**

Abstrak−Keamanan data sangat penting untuk melindungi informasi pribadi dan sensitif. Kasus kebocoran data yang pernah terjadi di Indonesia tercatat bahwa 80% data warga Indonesia dijual di forum gelap (dark web), hal ini tentu akan menimbulkan kerugian bagi individu maupun organisasi. Faktor yang menjadi penyebab kebocoran data bisa dari kurangnya protokol keamanan, serangan langsung, ataupun serangan phishing. Salah satu jenis serangan phishing yang menargetkan individu yang lebih spesifik disebut dengan spear phishing attack. Penelitian ini bertujuan untuk mengidentifikasi potensi kebocoran data dari data publik di instansi publik dengan merumuskan attack tree berdasarkan Data Flow Diagram (DFD) dari spear phishing attack menggunakan metrik granularitas data dengan kombinasi serangan dari Open Source Intelligence (OSINT) tools, social engineering tools, dan email spoofing. Penelitian ini menghasilkan dan membandingkan empat model attack tree dengan tidak sampai pada attack launching atau eksploitasi. Pertama OSINT TheHarvester, social engineering SEToolkit, dan email spoofing. Ke dua OSINT Metagoofil, social engineering ZPhisher, dan email spoofing. Ke tiga OSINT Recon-ng, social engineering SEToolkit, dan email spoofing. Ke empat OSINT Snov.io, social engineering ZPhisher, dan email spoofing. Spear phishing attack menggunakan OSINT Snov.io merupakan kombinasi serangan terbaik dikarenakan memiliki rincian data yang bervariasi yaitu mendapatkan lima jenis data dan tingkat granularitas data yang tinggi dengan jumlah data 367 sehingga semakin banyak peluang untuk melakukan perencanaan serangan dan analisis keamanan.

Kata Kunci: Spear Phishing Attack; Social Engineering; Open Source Intelligence (OSINT); Attack Tree; Metrik Granularitas Data

Abstract−Data security is important to protect personal and sensitive information. Data leakage cases that have occurred in Indonesia have recorded that 80% of Indonesian citizens' data is sold on dark forums (dark web), this will certainly cause losses to individuals and organizations. Factors that cause data leaks can be the lack of security protocols, direct attacks, or phishing attacks. One type of phishing attack that targets more specific individuals is called a spear phishing attack. This research aims to identify potential data leakage from public data in public institutions by formulating an attack tree based on the Data Flow Diagram (DFD) of a spear phishing attack using data granularity metrics with a combination of attacks from Open Source Intelligence (OSINT) tools, social engineering tools, and email spoofing. This research generates and compares four attack tree models with no attack launching or exploitation. First OSINT TheHarvester, social engineering SEToolkit, and email spoofing. Second OSINT Metagoofil, social engineering ZPhisher, and email spoofing. Third OSINT Recon-ng, social engineering SEToolkit, and email spoofing. The fourth OSINT Snov.io, social engineering ZPhisher, and email spoofing. Spear phishing attack using OSINT Snov.io is the best attack combination because it has varied data details, namely getting five types of data and a high level of data granularity with a total of 367 data so that there are more opportunities to carry out attack planning and security analysis.

Keywords: Spear Phishing Attack; Social Engineering; Open Source Intelligence (OSINT); Attack Tree; Data Granularity Metric

1. PENDAHULUAN

Teknologi sistem informasi yang semakin maju memberikan kemudahan suatu organisasi ataupun individu untuk menyimpan, mengolah, dan menyebarkan data ke publik sehingga dapat diakses oleh siapa saja[1]. Hal ini menjadikan keamanan data menjadi hal utama yang harus diperhatikan untuk melindungi data menyangkut informasi pribadi dan sensitif didalamnya [2]. Untuk menjaga keamanan data dari kebocoran data diperlukan prosedur pengelolaan keamanan yang baik [3]. Keamanan siber yang baik dapat dilakukan dengan tindakan memastikan keamanan dari alat, aset informasi, ataupun suatu sistem dari ancaman keamanan [4]. Ancaman keamanan yang seringkali terjadi biasanya dikarenakan penyerang memanfaatkan celah penggunaan dari teknologi informasi [5].

Salah satu celah keamanan yang bisa menjadi ancaman kebocoran data yaitu kurangnya kesadaran individu akan serangan yang mungkin terjadi dengan memanipulasi korban biasanya melalui email phishing attack. Phishing attack merupakan serangan yang dilakukan untuk mencoba mendapatkan informasi sensitif dengan mengirimkan email yang berisikan link yang dapat mengarahkan korban pada halaman website palsu [6], biasanya penyerang akan menggunakan teknik manipulasi (social engineering) yang dapat mendesak korban untuk mengakses link tersebut dan mendapatkan informasi rahasia korban [7]. Menurut penelitian Arizal, berdasarkan pada laporan Cost of Data Breach Report 2021 yang disusun oleh International Business Machines (IBM) phishing attack merupakan salah satu dari sepuluh attack vectors yang menempati posisi ke dua dengan 17% yang berarti phishing attack masih digunakan penyerang untuk mencuri data [8].

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

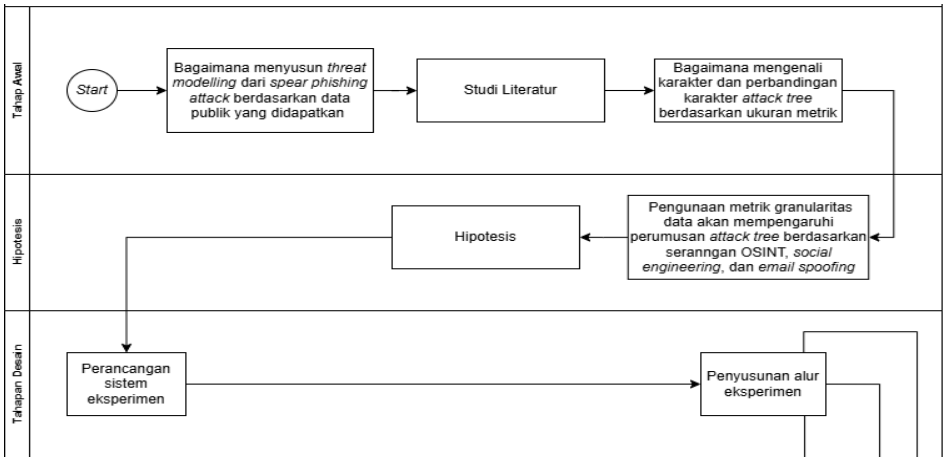
Kondisi ini perlu menjadi perhatian pada instansi publik dikarenakan Indonesia pernah mengalami kebocoran data dengan kerugian mencapai sekitar 600 triliun rupiah dimana terdapat 80% data warga Indonesia didalamnya yang tersebar pada aplikasi dan website yang pastinya menyimpan banyak data pribadi seperti informasi pegawai, informasi aset terenkripsi, dan informasi identitas pengguna [9]. Data pribadi yang merupakan aset yang harus dilindungi oleh suatu organisasi maupun individu dikarenakan berisikan data pribadi yang bersifat privasi dengan tujuan agar tidak disalahgunakan oleh pihak yang tidak berkepentingan yang dapat menyebabkan kerugian [10]. Kerugian yang dapat dirasakan bagi organisasi apabila mengalami kebocoran data dapat menurunkan kepercayaan publik, penyalahgunaan identitas, dan kerugian finansial. Oleh karena itu, diperlukan adanya pengujian keamanan terhadap perlindungan data di instansi publik. Penelitian ini akan melakukan percobaan pengujian dengan salah satu jenis phishing attack yaitu spear phishing attack dengan memanfaatkan data publik sebagai target. Spear phishing attack merupakan penyerangan pengiriman email yang menargetkan individu lebih spesifik [11], . Dengan menggunakan metode Open Source Intelligence (OSINT) tools untuk mengetahui kerentanan dengan mendapatkan data secara publik [12]. Selain itu, memanfaatkan serangan social engineering tools untuk memanipulasi psikologis target untuk mengirimkan email spoofing. Email spoofing akan berperan untuk mengirimkan konten email yang dibuat seolah email tersebut asli atau sah [13].

Penelitian yang dilakukan Khairunnisa, dkk (2024), menghasilkan bahwa semua media sosial yang berhasil diuji memiliki kerentanan terhadap serangan phishing dengan menggunakan Zphisher dan Social Engineering Toolkit (SET) dengan metode pengiriman email spoofing [10]. Penelitian yang dilakukan I Putu Agus Eka Pratama (2023), menghasilkan penilaian risiko berdasarkan framework ISO 31000:2018 dan menyusun rekomendasi dari hasil pengujian menggunakan tool OSINT theHarvester pada Bali Smart Island [14]. Penelitian yang dilakukan Ni Komang, dkk (2023), menghasilkan perbedaan dan perbandingan dari kecepatan akses, instalasi, akurasi, dan efektivitas dari penggunaan tools Zphisher, Shellphish, serta Whphisher untuk melakukan serangan phishing [15]. Penelitian yang dilakukan Sri, dkk (2022), menghasilkan bahwa teknik manipulasi dapat dilakukan untuk melakukan serangan phishing sampai dengan mengirimkan email spoofing menggunakan Gmail dan bantuan tools Black Eye dan SET [16]. Penelitian yang dilakukan Ahmadian, dkk (2021), menghasilkan bahwa dengan menggunakan SET berhasil melakukan percobaan serangan phishing dengan membuat halaman login Twitter serta memberikan rekomendasi pencegahaannya [17]. Berdasarkan penelitian terdahulu penelitian ini akan berfokus pada analisis perbandingan pemodelan attack tree dari spear phishing attack berdasarkan metrik granularitas data dengan kombinasi percobaan serangan menggunakan OSINT tools, social engineering tools, dan email spoofing pada instansi publik tahapan pengujian akan disusun dengan Data Flow Diagram (DFD). Data Flow Diagram (DFD) merupakan diagram yang akan menggambarkan sebuah aliran informasi yang digunakan sebagai data masukkan (input) dan data keluaran (output) [18]. Pemodelan attack tree yang dibuat akan menggambarkan hubungan sebuah serangan dengan simpul-simpul yang mempresentasikan sub serangan [19]. Dengan merumuskan threat modeling menggunakan attack tree dapat digunakan untuk mengevaluasi spear phishing attack yaitu dengan membandingkan hasil pengujian dengan metrik yang diukur. Penelitian ini bertujuan untuk mengidentifikasi karakteristik ancaman mendatang yang lebih mendalam, serta dapat memberikan wawasan yang terstruktur dalam memahami pola serangan berdasarkan metrik yang digunakan pada attack tree.

2. METODOLOGI PENELITIAN

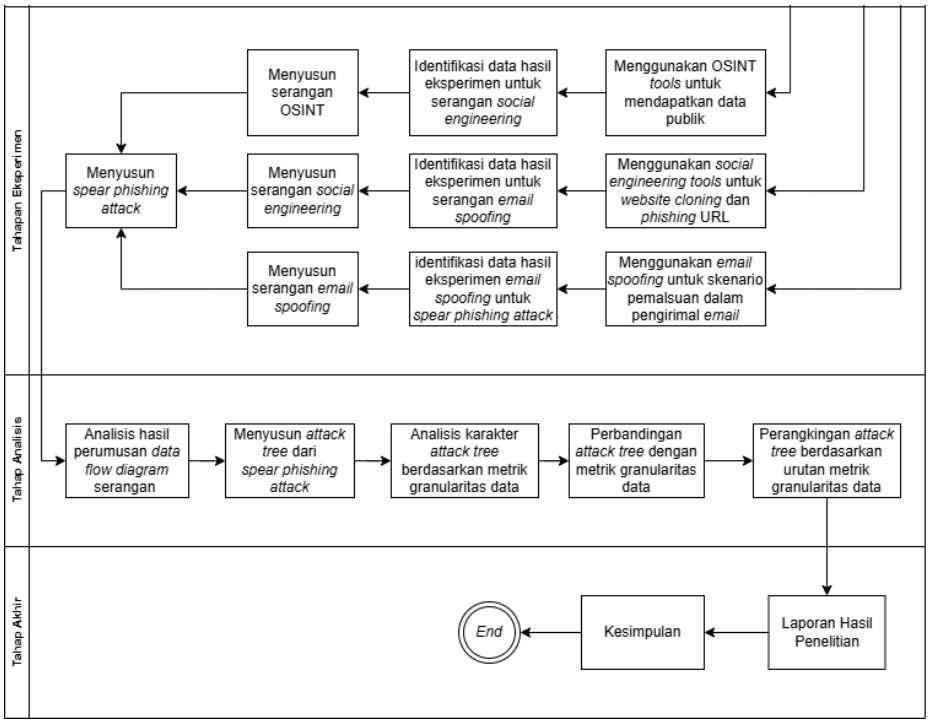
2.1 Sistematika Penelitian

Sistematika penelitian akan disajikan dalam bentuk alur yang tersusun dan akan menjadi panduan dalam memecahkan permasalahan yang ada di penelitian ini. Terdapat enam tahapan pada sistematika penelitian dapat dilihat pada Gambar 1 dan Gambar 2 sebagai berikut:



Gambar 1. Sistematika Penelitian

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876



Gambar 2. Lanjutan Sistematika Penelitian

1. Tahap Awal
   Tahap awal penelitian diawali dengan melakukan identifikasi tentang bagaimana menyusun threat modeling dari spear phishing attack berdasarkan data publik yang didapatkan. Dilanjutkan dengan melakukan riset berkaitan dengan studi literatur. Studi literatur dilakukan untuk memastikan masalah yang diangkat memiliki relevansi dan memungkinkan untuk dilakukan penelitian. Pengujian dengan melakukan eksperimen dilakukan setelah tahapan studi literatur telah dilakukan. Eksperimen dilakukan berkaitan dengan bagaimana mengenali karakter dan perbandingan attack tree berdasarkan dengan ukuran metrik yang digunakan yaitu metrik granularitas data. Pengukuran metrik granularitas data merupakan pengukuran yang mengacu pada tingkat detail yang dapat diamati dalam sekumpulan data diantaranya skala maupun jenis data. Semakin tinggi tingkat granularitas, maka akan semakin rinci dan mendalam dalam melakukan penelitian ataupun analisis [20].
2. Tahap Hipotesis
   Pada tahap hipotesis ini dilakukan proses praduga atau pernyataan sementara. Hipotesis menghasilkan pernyataan sementara yaitu penggunaan metrik granularitas data akan mempengaruhi perumusan serangan attack tree berdasarkan serangan OSINT, social engineering, dan email spoofing.
3. Tahap Desain
   Pada tahap ini berfokus pada tahap persiapan desain yang menyangkut perancangan eksperimen yaitu spesifikasi perangkat keras, spesifikasi perangkat lunak, platform eksperimen, dan daftar IP Address yang digunakan. Penyusunan alur eksperimen dibuat setelah perangkat lunak pada mesin virtual yaitu VM Kali Linux sebagai penyerang.
4. Tahap Eksperimen
   Pada tahap ini akan dilakukan eksperimen menggunakan OSINT tools untuk mendapatkan data publik, menggunakan social engineering tools untuk cloned website dan URL phishing, dan menggunakan email spoofing untuk skenario pemalsuan dalam pengiriman email yang nantinya akan menghasilkan data hasil eksperimen yang akan diidentifikasi untuk serangan. Data yang dihasilkan yaitu:
   a. Data hasil eksperimen berdasarkan OSINT tools untuk serangan social engineering.
   b. Data hasil eksperimen berdasarkan social engineering tools untuk serangan email spoofing.
   c. Data hasil eksperimen email spoofing untuk spear phishing attack.

   Eksperimen berhasil dilakukan dapat menyusun serangan yaitu menyusun serangan OSINT, menyusun serangan social engineering, dan menyusun serangan email spoofing. Setelah itu, dapat disusun menjadi spear phishing attack.
5. Tahap Analisis
   Pada tahap ini akan dilakukan analisis hasil perumusan data flow diagram berdasarkan serangan yang kemudian dapat disusun menjadi attack tree dari spear phishing attack. Selanjutnya dapat dilakukan analisis karakter yang akan digambarkan dengan attack tree diagram. Karakteristik attack tree akan dianalisis berdasarkan dengan data yang didapatkan dengan mempertimbangkan metrik granularitas data yang digunakan. Hasil analisis akan menunjukkan karakteristik dari masing-masing attack tree yang berkaitan

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

dengan metrik granularitas data. Kemudian akan dilakukan analisis perbandingan yang digunakan untuk menyusun pola attack tree berdasarkan dengan kondisi model serangan serangan yang dibuat. Setelah itu, hasil data yang dibandingkan akan diolah dengan melakukan pengkategorian berdasarkan ukuran metrik granularitas data.

6. Tahap Akhir

Tahap akhir merupakan tahap terakhir dari penelitian. Tahap ini dilakukan setelah adanya hasil analisis, dengan adanya hasil analisis maka dapat menghasilkan output berupa laporan penelitian. Setelah itu, penarikan kesimpulan terkait penelitian ini akan dilakukan berdasar pada hasil eksperimen dan hasil analisis mengenai karakteristik pada masing-masing attack tree.

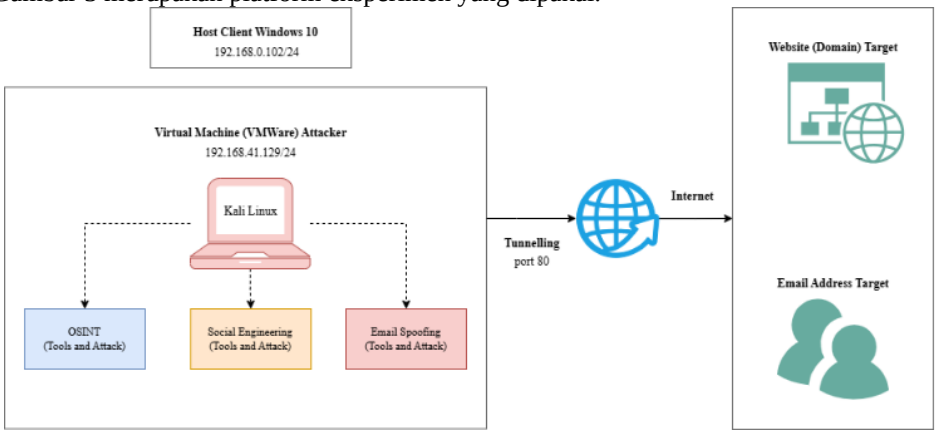
3. HASIL DAN PEMBAHASAN

3.1 Perencanaan dan Persiapan

Perencanaan dan persiapan merupakan tahapan penting yang dilakukan penyerang sebelum melakukan eksperimen dan serangan pada target. Pada tahap ini, untuk dapat mencapai tujuan penelitian dari eksperimen spear phishing attack menggunakan OSINT tools, social engineering tools, sampai dengan mengirimkan email spoofing menggunakan telnet diperlukan platform eksperimen dan perangkat lunak untuk membantu dalam penelitian. Lingkup pada penelitian ini yaitu Kali Linux, OSINT tools, Social Engineering tools, dan telnet sebagai sarana eksperimen.

a. Platform Eksperimen

Platform eksperimen dibuat untuk mengetahui perangkat yang akan dipakai dan menciptakan sebuah environment yang dirancang untuk melakukan eksperimen pengujian pada suatu domain dengan tujuan untuk mengidentifikasi kerentanan dari data publik yang mungkin dapat menjadi awal dari suatu serangan keamanan. Berikut Gambar 3 merupakan platform eksperimen yang dipakai.



Gambar 3. Platform Eksperimen

Pada Gambar 3 menjelaskan tentang perangkat dan layanan yang lebih detail. Pada penelitian ini platform eksperimen meliputi Internet, Main OS, virtual machine Kali Linux sebagai penyerang serta domain (website) dan email address target yaitu dari intansi publik sebagai objek penelitian. Target dapat diakses menggunakan tunneling dan internet. Tunneling yang terhubung ke Main OS berperan untuk memberikan jalan pada pengiriman email spoofing untuk dapat diakses di internet. Internet akan memberikan konektivitas untuk mengakses domain (website) target. Main OS memiliki sistem operasi Windows yang terdapat virtual machine Kali Linux yang berperan sebagai penyerang yang dapat melakukan serangan OSINT, serangan social engineering, dan serangan email spoofing kepada objek penelitian.

b. Spesifikasi Perangkat Lunak

Tabel 1 merupakan tabel yang menjelaskan spesifikasi perangkat lunak yang digunakan sebagai alat mengumpulkan informasi yang tersedia secara publik untuk menganalisis kerentanan kebocoran data. Perangkat lunak yang digunakan selama proses eksperimen pada penelitian adalah operating system, OSINT tools, social engineering tools, email spoofing, URL masking, dan tunneling service. Berikut merupakan rincian perangkat lunak yang digunakan:

Tabel 1. Spesifikasi Perangkat Lunak

Tipe	Software
Operating System	Kali Linux
OSINT Tools	theHarvester Metagoofil Recon-ng

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

Tipe	Software
Social Engineering Tools	Snov.io
	SEToolkit
	Zphisher
Tunneling Service	Ngrok
Email Spoofing	Telnet
URL Masking	Facad1ng

Pada Tabel 1 disebutkan beberapa spesifikasi perangkat lunak yang digunakan pada percobaan dan pengujian penelitian. Namun, sebelumnya sudah dilakukan percobaan penggunaan OSINT tools dan social engineering tools dengan total 13 tools dengan 6 tools yang tidak digunakan karena memiliki keterbatasan data yang dihasilkan atau terdapat error pada tools. Tools yang tidak digunakan yaitu Goofile, Recon-ng, Google dork, Profil3r, Hunter.io, Shodan.io, dan PyPhiser.

3.2 Data Hasil Eksperimen

Data hasil eksperimen bertujuan untuk menyajikan data yang didapatkan dari hasil implementasi eksperimen dengan menampilkan masukkan yang diproses oleh sistem dan data output merupakan hasil dari data input berupa target domain yang berhasil diproses. Setelah itu, data output yang didapatkan akan diidentifikasi, sehingga dapat menentukan data mana saja yang dapat dimanfaatkan untuk melakukan spear phishing attack oleh penyerang.

a. Data Hasil Eksperimen OSINT tool TheHarvester
Berdasarkan Tabel 2 setelah proses eksperimen menggunakan OSINT tool theHarvester selesai akan menghasilkan data output berupa ASN, URL, IP Address, Email, dan Host.

Tabel 2. Data Hasil Eksperimen OSINT tool TheHarvester

Input (Command)	Output				
	ASN	URL	IP	Email	Host
theHarvester -d [target domain] -l 300 -b all	AS*****	http://ggg.vv.yy	10.*.*.*	ju**@ ggg.vv.yy	a**. ggg.vv.yy :26.*.*.*
	AS*****	http://e*.*.vv.yy	25.*.*.*	se**@ ggg.vv.yy	a*. ggg.vv.yy :112.*.*.*
	AS****	http://fa*.*.vv.yy	23.*.*.*	w**@ ggg.vv.yy	a*.**. ggg.vv.yy

Pada Tabel 2 merupakan beberapa data yang ditampilkan dari keseluruhan data yang didapatkan. Diketahui keseluruhan data yang didapatkan berupa ASN sebanyak 5, URL sebanyak 39, IP sebanyak 57, email sebanyak 10, dan host sebanyak 155. Sehingga, total keseluruhan data yang didapatkan yaitu 266 data.

b. Data Hasil Eksperimen OSINT tool Metagoofil
Berdasarkan Tabel 3 setelah proses eksperimen menggunakan OSINT tool Metagoofil selesai akan menghasilkan data output berupa PDF file.

Tabel 3. Data Hasil Eksperimen OSINT tool Metagoofil

Input (Command)	Output
	PDF file
metagoofil -d [target domain]-t pdf -l 100 -n 100	https://ggg.vv.yy /ggg/**documents/203***.pdf https://ggg.vv.yy /ggg/**documents/725***.pdf https://www.ggg.vv.yy /ggg/**documents/27a***.pdf

Pada Tabel 3 merupakan beberapa data yang ditampilkan dari keseluruhan data yang didapatkan. Diketahui total keseluruhan PDF file yang didapatkan yaitu 69 file. PDF file yang didapatkan setelah diidentifikasi oleh penyerang diketahui mendapatkan sebanyak 29 emails.

c. Data Hasil Eksperimen OSINT tool Recon-ng
Berdasarkan Tabel 4 setelah proses eksperimen menggunakan OSINT tool Recon-ng selesai akan menghasilkan data output berupa IP Address dan Host.

Tabel 4. Data Hasil Eksperimen OSINT tool Recon-ng

Input (Command)		Output	
Module	Domain	IP Address	Host
Hackertarget	ggg.vv.yy	26.*.*.*	ggg.vv.yy
		112.*.*.*	ap**. ggg.vv.yy
		220.*.*.*	d***. ggg.vv.yy

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

Pada Tabel 4 merupakan beberapa data yang ditampilkan dari keseluruhan data yang didapatkan dengan module hacktertarget. Diketahui data yang didapatkan berupa IP Address sebanyak 36 dan host sebanyak 36. Sehingga, total keseluruhan data yang didapatkan yaitu 72 data.

d. Data Hasil Eksperimen OSINT tool Snov.io
Berdasarkan Tabel 5 setelah proses eksperimen menggunakan OSINT tool Snov.io selesai akan menghasilkan data output berupa emails, name, job position, location, dan LinkedIn.

Tabel 5. Data Hasil Eksperimen OSINT tool Snov.io

Input	Output				
	Emails	**Name**	**Job Position**	**Location**	**LinkedIn**
ggg.vv.yy	d***@ ggg.vv.yy	A*** D**	D*** O*** o* H**	Y******	https://www.linkedin.com/yy/d***-00****
	m***@ ggg.vv.yy	K*** M*** R****	P*** R**** R*** & H***	L*****	https://www.linkedin.com/yy/m***-r***-00***
	r***@ ggg.vv.yy	C*** R**	R*** I**** a** C****** H****	N****	https://www.linkedin.com/yy/r***-00*****

Pada Tabel 5 merupakan beberapa data yang ditampilkan dari keseluruhan data yang didapatkan. Diketahui data yang didapatkan berupa name sebanyak 106, job position sebanyak 58, emails sebanyak 106, location sebanyak 39, dan LinkedIn sebanyak 58. Total keseluruhan data yang didapatkan yaitu 367 data.

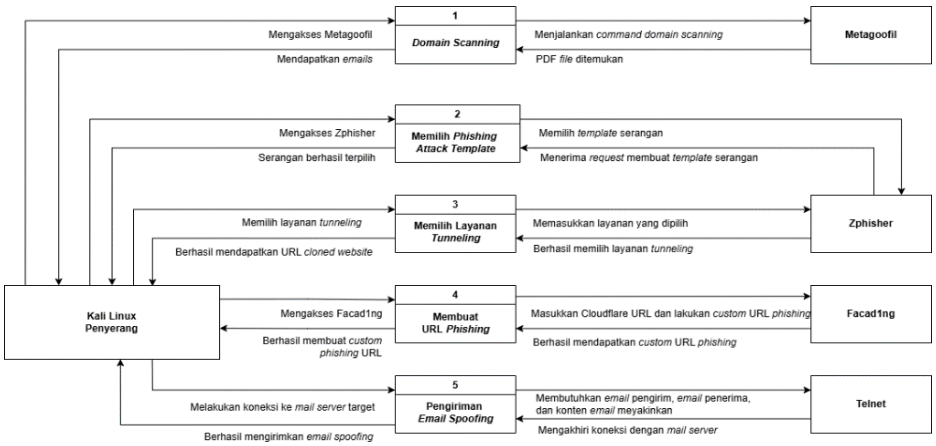
e. Data Hasil Eksperimen Social Engineering tool SEToolkit dan Zphisher
Setelah proses eksperimen menggunakan social engineering tool SEToolkit dan Zphisher selesai akan menghasilkan output berupa cloned website.

f. Data Hasil Eksperimen Pengiriman Email Spoofing
Setelah proses membuat cloned website menggunakan social engineering tool SEToolkit dan Zphisher pada target instansi publik sehingga berhasil mendapatkan URL phishing, maka penyerang dapat melakukan tahap selanjutnya dengan mengirimkan email spoofing menggunakan telnet.

3.3 Perumusan Data Flow Diagram dari Spear Phishing Attack

Perumusan serangan akan diolah dan didokumentasikan untuk menggambarkan alur proses spear phishing attack. Proses ini akan mencakup teknik mengumpulkan data dengan serangan OSINT, teknik memanipulasi psikologis target untuk mendapatkan data tertentu dengan serangan social engineering, dan teknik menyamarkan email pengirim sehingga email terlihat dari sumber yang terpercaya untuk mengeksploitasi target dengan serangan email spoofing. Perumusan serangan akan digambarkan dengan data flow diagram untuk memberikan informasi secara visual berupa data input dan data output. Tahapan ini merupakan bagian dari Proof of Concept (PoC) bertujuan untuk menunjukkan implementasi pada setiap proses spear phishing attack.

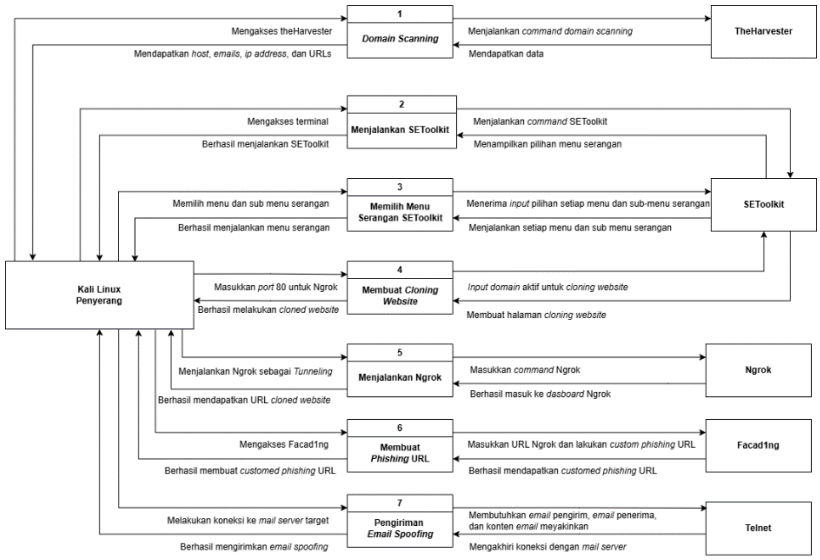
a. Hasil Perumusan Data Flow Diagram dari Spear Phishing Attack Berdasarkan Serangan OSINT Metagoofil, Social Engineering Zphisher, dan Email Spoofing
Pada hasil perumusan spear phishing attack ini data flow diagram dibuat berdasarkan serangan OSINT dengan Metagoofil, social engineering dengan Zphisher, dan email spoofing dengan telnet yang akan menggambarkan aliran data bagaimana spear phishing attack diimplementasikan. Berdasarkan Gambar 4 dapat dijelaskan proses yang berjalan hingga spear phishing attack dijalankan:



Gambar 4. Hasil Perumusan Spear Phishing Attack Berdasarkan Serangan OSINT Metagoofil, Social Engineering Zphisher, dan Email Spoofing

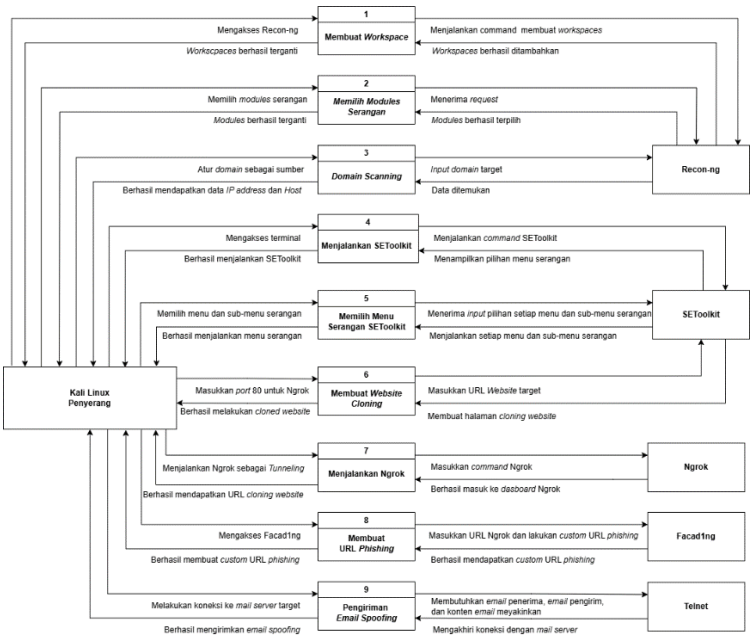
Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

b. Hasil Perumusan Data Flow Diagram dari Spear Phishing Attack Berdasarkan Serangan OSINT TheHarvester, Social Engineering SEToolkit, dan Email Spoofing
Pada hasil perumusan spear phishing attack ini data flow diagram dibuat berdasarkan serangan OSINT dengan theHarvester, social engineering dengan SEToolkit, dan email spoofing dengan telnet yang akan menggambarkan aliran data bagaimana spear attack diimplementasikan. Berdasarkan Gambar 5 dapat dijelaskan proses yang berjalan hingga spear phishing attack dijalankan:



Gambar 5. Hasil Perumusan Spear Phishing Attack Berdasarkan Serangan OSINT TheHarvester, Social Engineering SEToolkit, dan Email Spoofing

c. Hasil Perumusan Data Flow Diagram dari Spear Phishing Attack Berdasarkan Serangan OSINT Recon-ng, Social Engineering SEToolkit, dan Email Spoofing
Pada hasil perumusan spear phishing attack ini data flow diagram dibuat berdasarkan serangan OSINT dengan Recon-ng, social engineering dengan SEToolkit, dan email spoofing dengan telnet yang akan menggambarkan aliran data bagaimana spear phishing attack diimplementasikan. Berdasarkan Gambar 6 dapat dijelaskan proses yang berjalan hingga spear phishing attack dijalankan:

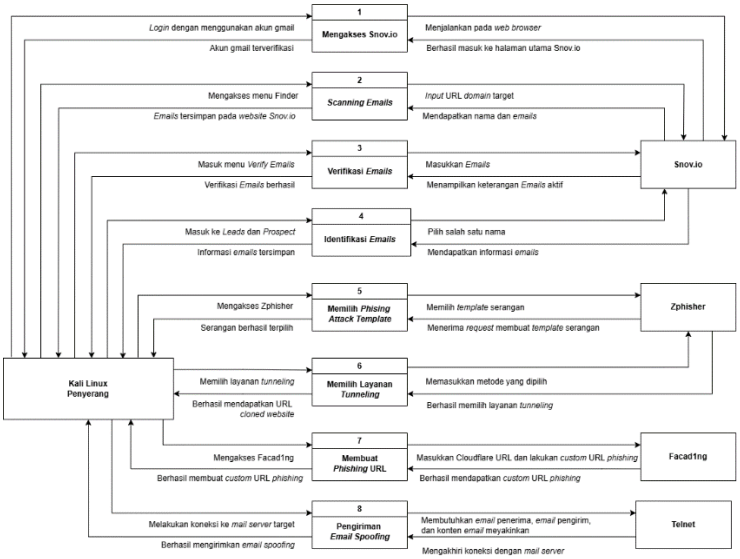


Gambar 6. Hasil Perumusan Spear Phishing Attack Berdasarkan Serangan OSINT Recon-ng, Social Engineering SEToolkit, dan Email Spoofing

d. Hasil Perumusan Data Flow Diagram dari Spear Phishing Attack Berdasarkan Serangan OSINT Snov.io, Social Engineering Zphisher, dan Email Spoofing
Pada hasil perumusan spear phishing attack ini data flow diagram dibuat berdasarkan serangan OSINT dengan Snov.io, social engineering dengan Zphisher, dan email spoofing dengan telnet yang akan menggambarkan

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

aliran data bagaimana spear phishing attack diimplementasikan. Berdasarkan Gambar 7 dapat dijelaskan proses yang berjalan hingga spear phishing attack dijalankan:



Gambar 7. Hasil Perumusan Spear Phishing Attack Berdasarkan Serangan OSINT Snov.io, Social Engineering Zphisher, dan Email Spoofing

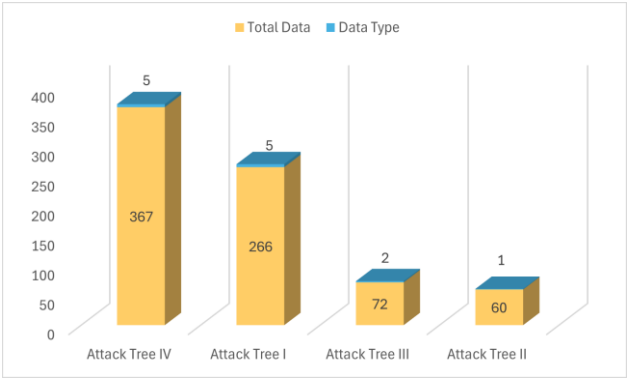
3.4 Analisis Perbandingan Attack Tree Berdasarkan Metrik Granularitas Data

Pengukuran granularitas dilakukan berdasarkan pernyerangan yang mengacu pada serangan yang memiliki nilai yang akan dihitung berdasarkan rincian data dan jumlah data yang didapatkan pada masa eksperimen. Berikut merupakan Tabel 6 yang menunjukkan nilai tingkat granularitas data dari serangan:

Tabel 6. Perbandingan Metrik Granularitas Data

Attack Tree	Kombinasi Serangan Spear Phishing	Jenis Data	Jumlah Data
Attack Tree I	Serangan OSINT theHarvester, Social Engineering SEToolkit, dan Email Spoofing	5	266
Attack Tree II	Serangan OSINT Metagoofil, Social Engineering Zphisher, dan Email Spoofing	1	60
Attack Tree III	Serangan OSINT Recon-ng, Social Engineering SEToolkit, dan Email Spoofing	2	72
Attack Tree IV	Serangan OSINT Snov.io, Social Engineering Zphisher, dan Email Spoofing	5	367

Pada Tabel 6 pengukuran dilakukan menggunakan dua metrik yaitu jenis data dan jumlah data. Pada penelitian ini akan diambil berdasarkan hubungan rincian data dan jumlah data yang didapatkan untuk menentukan granularitas data. Berdasarkan Tabel 6 dibuatkan diagram batang untuk menunjukkan perbandingan metrik granularitas data pada pengujian penyerangan spear phishing secara visual berdasarkan Gambar 8 sebagai berikut:



Gambar 8. Grafik Perbandingan Metrik Granularitas Data

Pada Gambar 8 dapat dijelaskan sumbu y mengarah vertikal menjelaskan rentang nilai dari jenis data dan jumlah data. Sementara sumbu x yang mengarah horizontal menjelaskan mengenai nama samaran penyerangan

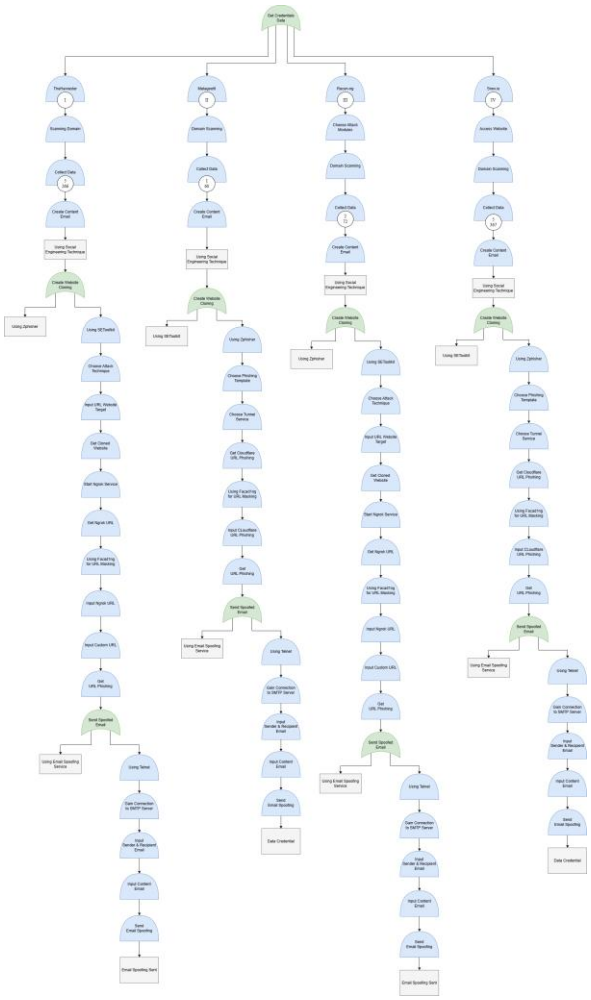
Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

pada pengujian pengukuran metrik granularitas data ini. Diagram batang berwarna biru disusun berdasarkan jenis data, sedangkan diagram batang berwarna oranye disusun berdasarkan jumlah data.
Berikut Tabel 7 merupakan pengurutan dari pengukuran metrik granularitas data pada pengujian spear phishing attack. Pengurutan disusun berdasarkan yang memiliki granularitas data dari yang tertinggi hingga yang terendah dari keseluruhan penyerangan yang diuji berdasarkan eksperimen sebagai berikut:

Tabel 7. Pengkategorian Metrik Granularitas Data Pada Attack Tree dari Spear Phishing Attack

Rank	Attack Tree	Jenis Data	Jumlah Data
1	Attack Tree I	5	266
2	Attack Tree II	1	60
3	Attack Tree III	2	72
4	Attack Tree IV	5	367

Pengkategorian dengan mengurutkan pada Tabel 7 dapat menyimpulkan bahwa pengujian serangan pada “Attack Tree IV” yaitu Spear Phishing Attack menggunakan OSINT Snov.io, Social Engineering Zphisher, dan Email Spoofing memiliki rincian data yang bervariasi yaitu lima jenis data dengan jumlah keseluruhan data yang didapatkan sebanyak 367 data sehingga ditempatkan pada urutan pertama. Sedangkan pengujian serangan pada “Attack Tree II” yaitu Spear Phishing Attack menggunakan OSINT Metagoofil, Social Engineering Zphisher, dan Email Spoofing dengan rincian data hanya dengan satu jenis data dan jumlah keseluruhan data yang didapatkan sebanyak 60 data sehingga ditempatkan pada urutan nomor 4 atau urutan terakhir. Setelah tahap pengujian dan pengukuran selesai dilakukan, pada penelitian ini dapat disimpulkan dengan sebuah gambar diagram attack tree yang menunjukkan tahap pengujian, proses data collecting, dan hasil dari data collecting yang dilakukan pada tiap serangan. Berdasarkan Gambar 9 berikut merupakan diagram attack tree dengan metrik granularitas data:



Gambar 9. Diagram Attack Tree dengan Metrik Granularitas Data

Pada Gambar 9 menjelaskan tentang attack tree diagram dari semua model serangan yang dibuat berdasarkan spear phishing attack. Semua serangan bertujuan untuk mendapatkan data kredensial dari target yang mengakses URL phishing. Pada diagram ini memuat empat model spear phishing attack yaitu Attack Tree I, Attack Tree II, Attack Tree III, dan Attack Tree IV yang masing-masing berisikan langkah dan pengukuran metrik

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

granularitas data dari awal hingga akhir. Pengukuran granulitas data pada masing-masing langkah pada attack tree berupa perhitungan jenis data dan jumlah data yang didapatkan dari hasil scanning. Sehingga nilai pengkategorian dapat dilihat pada model attack tree.

4. KESIMPULAN

Penelitian ini menghasilkan pemodelan spear phishing attack yang disusun dalam bentuk threat modeling berupa attack tree berdasarkan dengan data flow diagram dari setiap kombinasi serangan OSINT, serangan Social Engineering, dan serangan Email Spoofing. Attack tree ini dapat digunakan untuk memahami struktur dan relasi serangan. Metrik granuralitas data dapat digunakan untuk mengkategorikan berbagai macam model serangan. Berdasarkan 4 model serangan yaitu Attack Tree I kombinasi serangan OSINT theHarvester, social engineering SEToolkit, dan email spoofing mendapatkan lima jenis data dan jumlah data yang didapatkan sebanyak 266 data. Attack Tree II kombinasi serangan OSINT Metagoofil, social engineering Zphisher, dan email spoofing mendapatkan satu jenis data dan jumlah data yang didapatkan sebanyak 60 data. Attack Tree III kombinasi serangan OSINT Recon-ng, social engineering SEToolkit, dan email spoofing mendapatkan dua jenis data dan jumlah data yang didapatkan sebanyak 72 data. Serta, Attack Tree IV kombinasi serangan OSINT Snov.io, social engineering Zphisher, dan email spoofing mendapatkan lima jenis data dan jumlah data yang didapatkan sebanyak 367 data. Sehingga, berdasarkan 4 model kombinasi serangan yang dirumuskan dapat terlihat bahwa yang memiliki model spear phishing attack terbaik dapat dilihat dari tingkat granuralitas data tertinggi yaitu pada Attack Tree IV dikarenakan memiliki rincian data yang bervariasi dan tingkat granularitas data yang tinggi sehingga semakin banyak peluang untuk melakukan perencanaan serangan dan analisis keamanan.

REFERENCES

[1] Y. Yuliadarnita, M. Febriansyah, A. Wijaya, Y. Apridiansyah, dan R. Toyib, “Analisis Komparatif Aplikasi Open Source Intelligence Berbasis Website dengan Tools Osint Command Line Kominfo Bengkulu,” Jurnal Media Infotama, vol. 19, no. 2, hlm. 256–263, Okt 2023, doi: 10.37676/jmi.v19i2.3944.
[2] W. Febriyani, D. Fathia, A. Widjajarto, dan M. Lubis, “Security Awareness Strategy for Phishing Email Scams: A Case Study One of a Company in Singapore,” JOIV : International Journal on Informatics Visualization, vol. 7, no. 3, hlm. 808–814, Sep 2023, doi: 10.30630/joiv.7.3.2081.
[3] R. Milafebina, I. Putra Lesmana, dan M. R. Syailendra, “Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerence di Indonesia”, 2023, doi: https://doi.org/10.33648/jtm.v4i1.331.
[4] M. P. Aji, “Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective],” Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, vol. 13, no. 2, hlm. 222–238, Jan 2023, doi: 10.22212/jp.v13i2.3299.
[5] S. Parulian, D. A. Pratiwi, dan M. Cahya Yustina, “Ancaman dan Solusi Serangan Siber di Indonesia,” 2021
[6] M. A. B. Dewanto, M. Fathurrahman, D. R. Firdaus, dan A. Setiawan, “Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data,” Journal of Internet and Software Engineering, vol. 1, no. 4, hlm. 11, Jun 2024, doi: 10.47134/pjise.v1i4.2672.
[7] R. E. P. R. Palaloi dan R. Rahman, “Analisis dan Pencegahan Serangan Sosial Engineering Pada Jaringan Komputer Studi Kasus Penipuan Investasi Crypto,” Jurnal Riset Sistem Informasi, vol. 1, no. 3, hlm. 08–16, Jul 2024, doi: 10.69714/8b7xtv35.
[8] A. Arizal, Dendi Risman Saputra, dan Girinoto, “Investigasi Insiden Kebocoran Data Menggunakan Integrasi Melalui Pendekatan Open Source Intelligence dan Detection Maturity Level Model,” Info Kripto, vol. 17, no. 3, Des 2023, doi: 10.56706/ik.v17i3.86.
[9] H. B. Setiawan, & Fatma, dan U. Najicha, “Perlindungan Data Pribadi Warga Negara Indonesia Terkait dengan Kebocoran Data,” Jurnal Kewarganegaraan, vol. 6, no. 1, 2022.
[10] K. Z. Ansyafa, M. Fajarudin, M. Fadhil, dan S. N. Neyman, “Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit,” Journal of Internet and Software Engineering, vol. 1, no. 4, hlm. 10, Jun 2024, doi: 10.47134/pjise.v1i4.2641.
[11] Sutarti, Siswanto, dan A. Bachtiar, “Analisis Web Phishing Menggunakan Metode Network Forensic dan Block Access Situs dengan Router Mikrotik,” PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, vol. 10, no. 1, hlm. 71–83, Agu 2023, doi: 10.30656/prosisko.v10i1.7048.
[12] Yusuf Raharja, “Implementasi Metode Osint untuk Mengidentifikasi Serangan Judi Online pada Website,” Jurnal Informatika Polinema, vol. 10, no. 3, hlm. 359–364, Mei 2024, doi: 10.33795/jip.v10i3.4847.
[13] A. Harbani dan A. Sidiyantoro, “Implementasi Simple Mail Transfer Protocol Relay Pada Mail Gateway Untuk Menentukan Konten Email Spam,” Jurnal Ilmiah Teknologi-Informasi & Sains, vol. 12, hlm. 57–66, 2022, doi: 10.36350/jbs.v12i1.
[14] I. P. A. Pratama Eka, “Smart Security Risk Management pada Bali Smart Island menggunakan OSINT, OTGv4.2, dan ISO 310002018,” Jurnal Teknologi Informasi Komunikasi (e-Journal), vol. 10, 2023.
[15] N. K. A. T. Wahyuni, Putu Putri Cahayani, I Gusti Ngurah Yogi Wicaksana, dan Ida Ayu Kadek Bintang Wijayanti, “Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zphiser, Shellphish dan Whphisher,” Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, vol. 3, no. 1, hlm. 23–31, Mar 2023, doi: 10.55606/teknik.v3i1.915.

Journal of Information System Research (JOSH)
Volume 6, No. 3, April 2025, pp 1544−1554
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i3.5876

[16] S. Wahyuni, I. M. Raazi, dan I. Dwitawati, "Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 5, no. 1, hlm. 49–55, Feb 2022, doi: 10.32672/jnkti.v5i1.3962.
[17] H. Ahmadian dan A. Sabri, "Teknik Penyerangan Phishing Pada Social Engineering Menggunakan SET dan Pencegahannya," Djtechno Jurnal Teknologi Informasi, vol. 2, no. 1, hlm. 13–20, Jul 2021, doi: 10.46576/djtechno.v2i1.1251.
[18] M. Haidar Bagir, B. E. Putro, J. Pasir, dan G. Cianjur, "Analisis Perancangan Sistem Informasi Pergudangan di CV. Karya Nugraha," Jurnal Media Teknik & Sistem Industri, vol. 2, no. 1, hlm. 20–29, 2018
[19] L. Kuipers, "Analysis of Attack Trees: fast algorithms for subclasses," 2020.
[20] D. Cirillo, I. Núñez-Carpintero, dan A. Valencia, "Artificial intelligence in cancer research: learning at different levels of data granularity," Mol Oncol, vol. 15, no. 4, hlm. 817–829, Apr 2021, doi: 10.1002/1878-0261.12920.