Analisis *Stormbreaker* Sebagai Alat *Social Engineering* untuk Pemantauan pada Perangkat *Handphone* Berbasis *Website*

Lalu Arif Trasna Ashari, Lilik Widyawati, Kurniadin Abd Latif , Andi Sofyan Anas

Universitas Bumigora, Mataram, Indonesia

Correspondence : *e-mail*: laluarifta@gmail.com

Abstrak

Keamanan data dan privasi pengguna menjadi isu penting di era digital, terutama dengan meningkatnya teknik social engineering yang menyasar perangkat mobile. Salah satu potensi ancaman adalah penyalahgunaan data pribadi, akses kamera dan lokasi melalui halaman web. Permasalahan yang diangkat dalam penelitian ini adalah bagaimana menganalisis dan mengimplementasikan alat social engineering bernama STORMBREAKER untuk melakukan pemantauan jarak jauh terhadap perangkat handphone berbasis website secara real time. Tujuan dari penelitian ini adalah merancang sistem pengawasan berbasis web yang mampu merekam informasi sensitif seperti lokasi, kamera, dan data perangkat sebagai bentuk simulasi serangan social engineering. Penelitian ini menggunakan metode eksperimental dengan pendekatan simulasi. Penulis melakukan instalasi dan konfigurasi STORMBREAKER pada sistem Kali Linux. Pengujian dilakukan pada beberapa perangkat Android dan IOS dengan skenario penggunaan langsung dan simultan untuk melihat efektivitas sistem dari sisi teknis dan keamanan. Hasil pengujian menunjukkan bahwa STORMBREAKER mampu melakukan Capture secara real time, dengan hasil berbeda antar sistem operasi. Pada Android , proses Capture berjalan terus-menerus selama izin kamera aktif, sedangkan pada IOS hanya berjalan di awal dan Gambar menjadi statis. Implementasi STORMBREAKER terbukti efektif sebagai alat simulasi dalam pengujian dan edukasi keamanan siber, khususnya dalam mengidentifikasi celah keamanan dari sisi pengguna dan perangkat yang digunakan.

Kata kunci: *STORMBREAKER, social engineering, Android , IOS.*

Abstract

Data security and User privacy are important issues in the digital age, especially with the rise of social engineering techniques targeting mobile devices. One potential threat is the misuse of personal data, camera access, and location through web pages. The problem addressed in this study is how to analyze and implement a social engineering tool called STORMBREAKER to perform real-time remote monitoring of website-based mobile devices. The objective of this study is to design a web-based surveillance system capable of recording sensitive information such as location, camera, and device data as a form of social engineering attack simulation. This study employs an experimental method with a simulation approach. The author installed and configured STORMBREAKER on the Kali Linux system. Testing was conducted on several Android and IOS devices using direct and simultaneous usage scenarIOS to assess the system's effectiveness from both technical and security perspectives. The test results show that STORMBREAKER is capable of real-time capture, with different results across operating systems. On Android , the Capture process runs continuously while camera permissions are active, whereas on IOS, it only runs initially, and the image becomes static. The implementation of STORMBREAKER has proven effective as a simulation tool for cybersecurity testing and education, particularly in identifying security vulnerabilities from the User and device perspectives.

Keywords*: STORMBREAKER, social engineering, Android , IOS.*

1. Pendahuluan

Kemajuan pesat dalam teknologi dan aplikasi digital telah merangsang dan memungkinkan pertumbuhan dramatis dalam populasi pengguna global [1], terutama dalam komunikasi, bisnis, dan layanan publik [2]. Namun, kemajuan ini juga disertai meningkatnya ancaman keamanan siber[3]

Perubahan ini membawa pengaruh yang signifikan terhadap pola hidup manusia di era digital saat ini [4][5]. Salah satu bentuk serangan yang marak adalah *social engineering*, yakni manipulasi psikologis yang digunakan untuk mendapatkan akses ke informasi sensitif [6]. Ancaman ini bersifat lintas batas (borderless) dan dapat menyasar siapa saja, mulai dari masyarakat umum hingga tenaga ahli.

Website merupakan bagian dari internet yang dapat menampilkan teks, gambar, suara, dan video, serta memungkinkan suatu dokumen ditautkan ke dokumen lain menggunakan media akses browser [7]. Dengan sifatnya yang interaktif dan mudah diakses, website menjadi medium yang potensial bagi pelaku *social engineering* untuk melancarkan serangan secara real time dan jarak jauh [8].

Berbagai penelitian telah menyoroti aspek *social engineering* dan keamanan digital. [9] menekankan pada potensi ancaman, [10] menganalisis praktik phishing dengan *Social engineering* Toolkit (SET), sedangkan Zein [11] membahas urgensi kebijakan keamanan. [12] mempelajari penggunaan zphisher untuk simulasi serangan phishing, sementara [13] menekankan pentingnya edukasi masyarakat. Namun, sebagian besar penelitian masih terbatas pada kajian teoritis, belum banyak yang melakukan eksperimen teknis langsung dengan perangkat modern.

Penelitian ini hadir untuk mengisi kesenjangan tersebut dengan menganalisis dan menguji STORMBREAKER, alat *social engineering* berbasis *web* yang mampu mengakses kamera, mikrofon, lokasi, dan data perangkat target [14]. Alat ini dapat digunakan untuk simulasi serangan berbasis website secara *real time* [15]. Pertanyaan utama penelitian ini adalah: "Bagaimana analisis dan implementasi *STORMBREAKER* se-bagai alat *social engineering* untuk pemantauan jarak jauh pada perangkat handphone berbasis *website* secara *real time*?"

2. Metode Penelitian

2.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimen teknis berbasis simulasi dengan pendekatan deskriptif kuantitatif. Tujuan utama adalah mengidentifikasi dan mengevaluasi potensi *STORMBREAKER* dalam mengakses data perangkat melalui interaksi *web*.

2.2. Target, Etika, dan Validitas Simulasi

Simulasi dilakukan dengan target dummy (perangkat sendiri) tanpa melibatkan pengguna eksternal. Empat perangkat digunakan: *iPhone XR* 128GB, *iPhone XR* 64GB, *Samsung* A06, dan *Samsung* A55. Pengujian dilakukan dalam lingkungan *Windows Subsystem for Linux (WSL)* dengan *Kali Linux* 2024.3.

2.3. Alat dan bahan

Penelitian ini memanfaatkan berbagai perangkat lunak dan perangkat keras yang mendukung proses simulasi teknis secara maksimal. Adapun alat dan bahan yang digunakan dalam penelitian ini meliputi:

1. Kali Linux: Sistem operasi utama yang dirancang khusus untuk kegiatan pengujian keamanan jaringan dan forensik digital. *Kali Linux* dIPilih karena telah dilengkapi dengan berbagai *tools* bawaan.
2. *STORMBREAKER* : Storm-Breaker adalah alat rekayasa sosial yang dirancang untuk mengakses informasi *device* tanpa memerlukan izin dari pengguna, *web*cam, dan lokasi perangkat.
3. *Ngrok* dan Cloudflare: Layanan reverse proxy yang digunakan untuk mengekspos *server* lokal ke jaringan publik, menghasilkan *URL HTTP*/*HTTPS* sementara yang tampak sah di mata target.
4. Laptop/PC: Dengan spesifikasi mendukung virtualisasi atau dual-boot Kali Linux
5. Handphone: sebagai ujicoba *tools STORMBREAKER* .
6. Akun *Ngrok* dan *Cloudflare* aktif dan koneksi internet stabil: Diperlukan untuk menghubungkan *server* lokal ke jaringan luar.

2.4. Simulasi

Simulasi serangan dilakukan dalam beberapa tahapan sistematis menggunakan sistem operasi Kali Linux, *STORMBREAKER* , dan layanan *tunnel*ing *Ngrok* atau Cloudflare. Setiap langkah dilakukan dalam lingkungan virtual yang terkendali, melibatkan data pengguna asli. Berikut ini adalah ringkasan tahapan yang dilakukan dalam proses simulasi:

Tabel 1. Langkah-langkah Simulasi

NO	TAHAPAN	PENJELASAN
1	Installasi requirements dan *STORMBREAKER*	Menginstall requirements yang di butuhkan untuk menjalankan *STORMBREAKER*
2	Modifikasi kode	Memodifikasi kode menjadi tampilan situs penyedia film online
3	Konfigurasi proxy, repository dan *tunnel*ing	Autentikasi *Ngrok* dan *Cloudflare* untuk memulai koneksi aman.
4	Ekspos halaman menggunakan *Ngrok* dan Cloudflare	Mendapatkan *URL* publik *HTTPS* dari terminal.
5	Simulasi akses dan pencatatan	Masuk ke link di lakukan, dan data di tangkap otomatis di *web* Interface

Setiap langkah di atas dikontrol dengan cermat, dan hasil login dummy dari target diamati secara langsung melalui terminal Kali Linux, sebagaimana akan dijelaskan lebih lanjut pada bagian pengujian dan validasi hasil.

2.5. Diagram Alur Simulasi

Untuk memperjelas tahapan simulasi yang dilakukan, berikut disajikan diagram alur pelaksanaan penelitian. Diagram ini mengGambarkan proses mulai dari konfigurasi awal hingga pencatatan hasil pemantauan melalui *web* Interface.

Gambar 1. Diagram Alur Perancangan Integrasi STORMBREAKER

Diagram tersebut mengGambarkan bahwa setiap tahap dalam simulasi dilakukan secara berurutan dan terstruktur, dimulai dari konfigurasi awal alat hingga proses penangkapan data kredensial target. Dengan adanya visualisasi ini, diharapkan pembaca dapat memahami alur teknis pelaksanaan penelitian secara menyeluruh. Alur ini juga menunjukkan bahwa simulasi dilakukan secara sistematis, terkendali, dan etis, tanpa melibatkan pengguna aktual, sehingga hasil yang diperoleh tetap valid dan relevan.

2.6. Parameter Pengujian

Penelitian ini menggunakan beberapa parameter untuk mengukur keberhasilan simulasi yang dilakukan. Pengujian dilakukan dalam 4 handphone untuk memastikan hasil yang valid dan konsisten. Berikut adalah parameter yang digunakan:

Tabel 2. Parameter Pengujian dalam Simulasi *STORMBREAKER*

Parameter	Indikator Pengukuran
Cara kerja *STORMBREAKER*	Menganalisis cara kerja dari *STORMBREAKER* untuk mendapatkan akses kamera, lokasi, dan informasi device
Jumlah Capture	Mengukur berapa banyak hasil *Capture* yang di hasilkan dalam waktu 5 menit.

Akurasi Lokasi	Mengukur seberapa akurat fitur lokasi *tools STORMBREAKER* .
Informasi Device	Mengukur informasi yang akan di tampilkan *STORMBREAKER* : Informasi yang akan di dapatkan admin IP : os name : Version : *Browser* Name : GET *Browser* Version : CPU Name : Resolution : Time Zone : Language : Number Of CPU Core :
Kapasitas *Server*	Mengukur kapasitas *server* yang dapat menampung jumlah Capture.
Performa *Website*	Mengukur performance, Accessibility, dan Best Practices.
Respon dari Sistem Operasi	Mengukur sejauh mana keamanan sistem operasi *Android* dan *IOS* .
Cek Virus	Mengecek virus menggunakan *website virustotal*.
Respon dari Browser	Mengukur sejauh mana keamanan *Browser* di tambahkan dengan default, *VPN*, *Cloudflare* warp, dan private.

Parameter ini membantu menilai efektivitas serangan serta konsistensi hasil simulasi. Data yang diperoleh dari setiap sesi akan dibahas lebih lanjut pada bab berikutnya. Seluruh data yang diperoleh dari simulasi ini dianalisis secara kuantitatif untuk memastikan hasil yang objektif dan dapat direplikasi pada penelitian sejenis di masa mendatang.

3. Hasil dan Pembahasan

3.1. Sub judul Hasil Pemantauan *STORMBREAKER*

3.2.1 Kamera

a. Diberikan akses kamera

Tabel 3. pengujian hasil *Capture* device

No	Jumlah *Capture* ke *website* dalam waktu 5 menit		
	device	Secara Bergiliran	Bersamaan
1	*XR* 128	33	
2	*XR* 64	33	
3	*Samsung* a05	28	
4	*Samsung* a55	33	
Jumlah Capture		127	100

Pengujian dilakukan pada perangkat Android dan iOS dengan berbagai skenario. Pada perangkat Android, proses capture kamera berjalan terus-menerus selama izin akses aktif, sementara pada iOS, capture hanya dilakukan sekali pada pemberian izin awal. Namun, setelah dilakukan modifikasi kode pada file index.html di direktori camera_temp, STORMBREAKER berhasil melakukan capture berulang pada perangkat iOS. Pengujian kamera menunjukkan bahwa dalam waktu 5 menit, akses satu per satu perangkat menghasilkan 127 capture, sedangkan akses bersamaan dari 4 perangkat hanya menghasilkan 100 capture, yang mengindikasikan penurunan performa server sebesar 21,26% saat menangani banyak permintaan secara simultan.

Tabel 4. Hasil *Capture* Pada OS *IOS* dan *Android*

Perangkat *IOS XR* 64	Perangkat *IOS XR* 128	Perangkat *Android Samsung* a06	Perangkat *Android Samsung* a55
			
			
			
			
			

b. Tidak diberikan akses kamera

Gambar 13. tampilan eror pada console

Pada Gambar tampilan eror pada console saat tidak memberikan akses kamera pada template camera_temp

3.2.2 Lokasi

Lokasi adalah salah satu fitur utama dalam melakukan pemantauan menggunakan *tools* STORMBREAKER. Berikut merupakan beberapa device, *browser* yang digunakan untuk melakukan pemantauan dan tingkat akurasi yang didapatkan.

Tabel 4. Pengujian Akurasi Lokasi

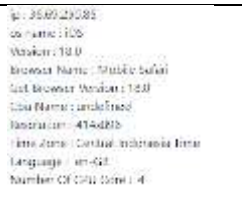
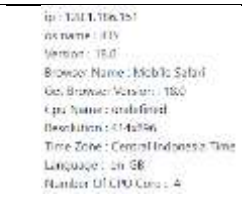
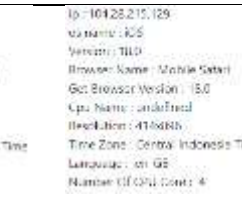
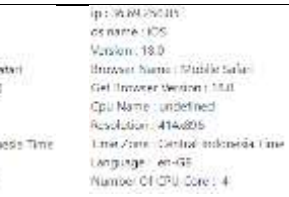
Handphone	Browser	Pengujian Cek akurasi lokasi		kesimpulan
		Lokasi Asli	Lokasi Hasil ***STORMBREAKER***	
IOS	*Browser* bawaan	8°35'13.5"S 116°07'11.1"E - Google Maps	*HTTPS*://google.com/maps/place/-8.587078759913071+116.1197396312492	Akurat
	UC		-	Tidak tersedia
	Chrome		*HTTPS*://google.com/maps/place/-8.587083781684132+116.11974031484702	Akurat
	Brave		*HTTPS*://google.com/maps/place/-8.587079361008174+116.11973952886504	akurat
	Opera mini		*HTTPS*://google.com/maps/place/-8.58708058964602+116.11973840764506	Akurat
Android	*Browser* bawaan	8°41'11.5"S 116°07'28.4"E - Google Maps	*HTTPS*://google.com/maps/place/-8.686518184986603+116.12454126115526	Akurat
	UC		The request to get user location timed out	Timed out
	Chrome		*HTTPS*://google.com/maps/place/-8.6865183207983+116.12454133531926	Akurat
	Brave		*HTTPS*://google.com/maps/place/-8.686518283849626+116.12454131508895	Akurat
	Opera mini		Google Map Link : https://google.com/maps/place/-8.686518291631089+116.12454131936593	Akurat
			HTTPS://google.com/maps/place/-8.686518291631089+116.12454131936593	

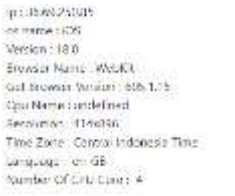
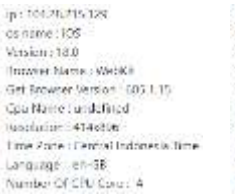
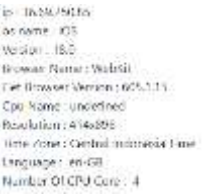
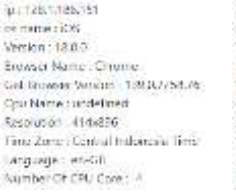
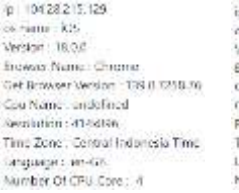
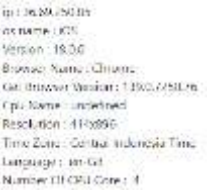
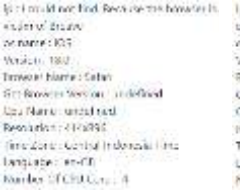
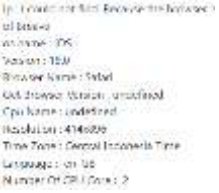
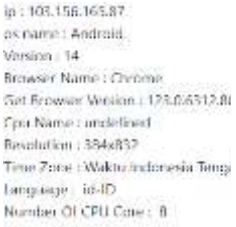
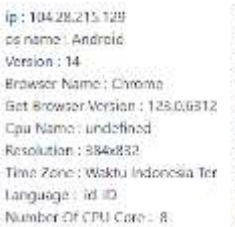
Pada merupakan hasil dari beberapa pengujian dari akurasi dari *tools STORMBREAKER*, yang mendapatkan hasil yang sudah akurat, namun pada *browser* UC request permission akses lokasi tidak muncul di sistem operasi *IOS* dan pada *Android* muncul tetapi tidak dapat memberikan lokasi yang akurat, dalam *panel.PHP* menampilkan request lokasi *User* time out di karenakan oleh tidak memiliki service worker yang mengakibatkan tidak bisa mengakses DOM.

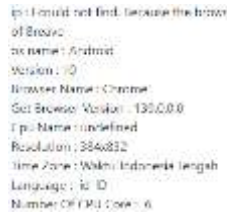
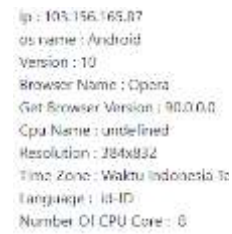
3.2.3 Pemantauan Browser

Informasi *device* adalah salah satu fitur utama dalam melakukan pemantauan menggunakan *tools* STORMBREAKER. Berikut merupakan beberapa device, *browser* yang digunakan untuk melakukan pemantauan dan hasil informasi yang di dapatkan dari *device* yang di gunakan.

Tabel 5. Hasil Pemantauan *Browser* Dari Sisi Admin

Perangkat	Browser	Default	Turbo *VPN*	Cloud Flare warp	Private
IOS	*Browser* bawaan				

	UC				
	Chrome				
	Brave				
	Opera mini	ip : 36.69.250.85 os name : iOS Version : 18.0 Browser Name : Mobile Safari Get Browser Version : 18.0 Cpu Name : undefined Resolution : 414x896 Time Zone : Central Indonesia Time Language : en-GB Number Of CPU Core : 4	ip : 120.1.186.151 os name : iOS Version : 18.0 Browser Name : Mobile Safari Get Browser Version : 18.0 Cpu Name : undefined Resolution : 414x896 Time Zone : Central Indonesia Ti Language : en-GB Number Of CPU Core : 4	ip : 104.28.215.129 os name : iOS Version : 18.0 Browser Name : Mobile Safari Get Browser Version : 18.0 Cpu Name : undefined Resolution : 414x896 Time Zone : Central Indonesia T Language : en-GB Number Of CPU Core : 4	ip : 36.69.250.85 os name : iOS Version : 18.0 Browser Name : Mobile Safari Get Browser Version : 18.0 Cpu Name : undefined Resolution : 414x896 Time Zone : Central Indonesia Ti Language : en-GB Number Of CPU Core : 4
Android	*Browser* bawaan	ip : 103.156.165.87 os name : Android Version : 10 Browser Name : Chrome Get Browser Version : 130.0.0.0 Cpu Name : undefined Resolution : 384x832 Time Zone : Waktu Indonesia Ten Language : id-ID Number Of CPU Core : 8	ip : 91.210.214.196 os name : Android Version : 10 Browser Name : Chrome Get Browser Version : 130.0.0.0 Cpu Name : undefined Resolution : 384x832 Time Zone : Waktu Indonesia Ic Language : id-ID Number Of CPU Core : 8	ip : 104.28.215.129 os name : Android Version : 10 Browser Name : Chrome Get Browser Version : 130.0.0.0 Cpu Name : undefined Resolution : 384x832 Time Zone : Waktu Indonesia Ie Language : id-ID Number Of CPU Core : 8	ip : 103.156.165.87 os name : Android Version : 10 Browser Name : Chrome Get Browser Version : 130.0.0.0 Cpu Name : undefined Resolution : 384x832 Time Zone : Waktu Indonesia Tir Language : id-ID Number Of CPU Core : 8
	UC				
	Chrome				

Brave				
Opera mini				

Pada table menunjukan analisis terhadap beberapa *browser* popular dengan menambahkan *VPN*, *Cloudflare* warp dan mode private. Mendapatkan hasil *Brave* walaupun secara default menempatkan privasi sebagai prioritas utama serta memblokir tracker dan Script berbahaya yang di lengkapi *HTTPS* only dan mode *tor*, dalam pengujian ini *tools STORMBREAKER* memanipulasi kode agar *browser Brave* tidak dapat menampilkan hasil dengan semestinya.

4. Kesimpulan

Adapun kesimpulan yang dapat di ambil berdasarkan hasil uji coba yang telah di lakukan adalah *STORMBREAKER* berhasil diimplementasikan sebagai alat *social engineering* berbasis *website* yang mampu melakukan pemantauan jarak jauh terhadap perangkat handphone secara *real time*, dengan menyajikan data lokasi, akses kamera, dan informasi perangkat melalui antarmuka *web*. Instalasi dan konfigurasi dijalankan melalui sistem operasi *Kali Linux* menggunakan *WSL* untuk virtualisasi dan diuji pada perangkat *Android* dan *IOS*. Hasil pengujian menunjukkan perbedaan perilaku sistem operasi, di mana *Android* memungkinkan proses *Capture* berjalan terus-menerus selama halaman aktif, sementara *IOS* hanya melakukan *Capture* satu kali saat izin pertama diberikan, namun setelah di modifikasi *tools STORMBREAKER* mampu melakukan *Capture* pada *IOS* . Hasil pengujian menunjukkan perbedaan *UC* tidak memiliki service worker yang mengakibatkan tidak bisa mengakses *DOM*, pada *Brave* terdapat manipulasi kode yang mengakibatkan hasil yang di tampilkan tidak semestinya, beberapa *browser* yang di uji tidak memberikan keamanan seperti *browser* tor desktop. Sistem mampu melakukan *Capture* otomatis dan menyimpannya ke direktori *server* dengan ukuran File yang konsisten dan akurasi lokasi yang tinggi. Penurunan performa *server* di pengaruhi oleh jumlah *User* yang masuk ke *website*. *STORMBREAKER* terbukti efektif digunakan sebagai alat simulasi dalam pengujian dan edukasi keamanan siber berbasis *website*.

Daftar Pustaka

[1] H. Haqqi and H. Wijayati, *Revolusi Industri 4.0 di Tengah Society 5.0: Sebuah Integrasi Ruang, Terobosan Teknologi, dan Transformasi Kehidupan di Era Disruptif*. 2019.

[2] Ananya Chittlangia, “Phishing Simulation and Analysis Report.” [Online]. Available: https://github.com/ananya-chittlangia/phishing-simulation-and-analysis

[3] G. Aparna, B. Vamshi Krishna, C. K. Reddy, K. Latha, and M. Akshitha, “Phishing Simulations,” vol. 9, no. 11, pp. 866–869, 2024, [Online]. Available: www.ijnrd.org

[4] I. Damiarto, Alfitri, and Moh. Mahrus, “Article in Jurnal Tana Mana,” *Artic. J. Tana Mana*, vol. Vol. 4 No., no. 1, pp. 1–3, 2023, [Online]. Available: https://ojs.staialfurqan.ac.id/jtm/

[5] Bart Lenaerts-Bergmans, “10 Types of Social Engineering Attacks and how to prevent them.” [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/

[6] B. D. Victor Benny Alexsius Pardosi and dan A. Y. V. Fifto Nugroho, *SISTEM KEAMANAN INFORMASI*. 2024.

[7] T. Asra, S. Nur Khasanah, and E. Rikardo Nainggolan, “Rancang Bangun Sistem Informasi Manajemen Restoran Berbasis Web Pada Warunk Upnormal,” *Reputasi J. Rekayasa Perangkat Lunak*, vol. 4, no. 2, pp. 110–119, 2023, doi: 10.31294/reputasi.v4i2.2428.

[8] H. Ahmadian and A. Sabri, "Teknik Penyerangan Phishing Pada Social Engineering Menggunakan Set Dan Pencegahannya," *Djtechno J. Teknol. Inf.*, vol. 2, no. 1, pp. 13–20, 2021, doi: 10.46576/djtechno.v2i1.1251.

[9] E. M. Safitri, A. Pratama, M. A. Furqon, I. R. Mukhlis, Agussalim, and A. Faroqi, "Interaction effect of system, information and service quality on intention to use and user satisfaction," *Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020*, pp. 92–97, 2020, doi: 10.1109/ITIS50118.2020.9321002.

[10] H. Ahmadian and A. Sabri, "Teknik Penyerangan Phishing Pada Social," *J. Inf. Technol. Res.*, vol. 2, no. 1, 2021.

[11] A. Zein, "Analisa Penyerangan untuk Cyber Security Social Engineering," *J. Inform. Univ. Pamulang*, vol. 8, no. 4, pp. 642–648, 2023, doi: 10.32493/informatika.v8i4.35931.

[12] K. Z. Ansyafa, M. Fajarudin, M. Fadhil, and S. N. Neyman, "Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 10, 2024, doi: 10.47134/pjise.v1i4.2641.

[13] Y. Hartiwi, Y. Arvita, M. Purnasari, and Nurhayati, "Sosialisasi Edukasi Bahaya dan Upaya Pencegahan Social Engineering Untuk Meningkatkan Keamanan Informasi," *J. Pengabdi. Masy. UNAMA*, vol. 3, no. 1, pp. 65–72, 2024.

[14] untrasecurity, "Stormbreaker." [Online]. Available: https://github.com/ultrasecurity/Storm-Breaker

[15] geeksforgeeks, "Storm Breaker - Social Engineering Tool in Linux." [Online]. Available: https://www.geeksforgeeks.org/linux-unix/storm-breaker-social-engineering-tool-in-linux/