JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

Analisis Potensi Kerentanan Terhadap Serangan Phishing Pada Website Sttsundermann.Siakadcloud.Com Menggunakan Simulasi Lingkungan Kali Linux Dan NGROK

Delvin krisnawati lahagu[1], Deprianus Zalukhu[2], Fasrian mauren niella Hura[3], Fatarolius Harefa[4], Putra barato telaumbanua[5], Ofelius Laia[6]

[1,2,3,4,5,6]Program Studi Teknologi Informasi, Universitas Nias, Gunungsitoli, Indonesia

e-mail**:** [1]delvinkrisnawatilhg@gmail.com [2]deprianuszalukhu679@gmail.com [3]Fasrianmaurenniellahura@gmail.com [4]fatarharefa@gmail.com [5] baratotelaumbanua@gmail.com [6*]ofeliuslaia@gmail.com
(*Email Corresponding Author: ofeliuslaia@gmail.com**)**

Received: June, 20, 2025 | Revision: June, 30, 2025 | Accepted: July, 01, 2025

Abstrak

Penelitian ini bertujuan untuk menganalisis potensi kerentanan terhadap serangan phishing pada website akademik *sttsundermann.siakadcloud.com* melalui simulasi teknis berbasis Kali Linux dan layanan tunneling Ngrok. Dengan memanfaatkan *Social Engineering Toolkit* (SET), peneliti berhasil mereplikasi halaman login situs asli dan menyajikannya secara daring menggunakan URL HTTPS sementara yang dihasilkan oleh Ngrok. Halaman tiruan tersebut dirancang menyerupai tampilan situs resmi, sehingga saat target memasukkan data login, informasi tersebut tersadap secara real-time melalui terminal Kali Linux. Penelitian ini menggunakan metode eksperimen dalam lingkungan terkendali, tanpa melibatkan pengguna aktual, untuk menguji efektivitas alat dan mengidentifikasi celah keamanan pada sistem informasi akademik. Hasil simulasi menunjukkan serangan phishing dapat dilakukan secara efisien dan berpotensi tinggi membahayakan keamanan data pengguna, terutama jika sistem tidak dilengkapi mekanisme proteksi tambahan seperti autentikasi multifaktor (MFA) atau verifikasi keamanan lainnya. Penelitian ini diharapkan menjadi acuan bagi institusi pendidikan tinggi dalam meningkatkan kesadaran sivitas akademika terhadap ancaman phishing serta mendorong penerapan standar keamanan siber yang komprehensif dan berkelanjutan.

Kata Kunci: Phishing, Kali Linux, Ngrok, *Social Engineering Toolkit*, Keamanan Siber

Abstract

This study aims to analyze potential vulnerabilities to phishing attacks on the academic website *sttsundermann.siakadcloud.com* through a technical simulation using the Kali Linux operating system and Ngrok tunneling service. Utilizing the *Social Engineering Toolkit* (SET), the researchers successfully replicated the original site's login page and presented it online using a temporary HTTPS URL generated by Ngrok. The mock page was designed to resemble the official site so that when the target entered login data, the information was intercepted in real-time via the Kali Linux terminal. The study employed an experimental method in a controlled environment, without involving actual users, to test the effectiveness of the tools and identify security gaps in the academic information system. The results indicate that phishing attacks can be executed efficiently and pose a significant threat to user data security, especially if the system lacks additional protection mechanisms such as multi-factor authentication (MFA) or other security verifications. This research is expected to serve as a reference for higher education institutions to raise awareness among the academic community about phishing threats and to promote the comprehensive and sustainable implementation of cybersecurity standards.

Keywords: Phishing, Kali Linux, Ngrok, *Social Engineering Toolkit*, Cybersecurity

1. PENDAHULUAN

Phishing merupakan salah satu bentuk serangan siber berbasis rekayasa sosial *(social engineering)* yang bertujuan untuk memperoleh informasi sensitif dari korban secara ilegal. Serangan ini umumnya dilakukan dengan menipu korban melalui media komunikasi digital seperti email, pesan instan, atau situs web palsu yang menyerupai situs resmi [1]. Dalam praktiknya, pelaku menyamar sebagai institusi atau entitas terpercaya untuk mendapatkan informasi seperti kata sandi, nomor rekening, atau identitas pribadi lainnya. Data tersebut kemudian disalahgunakan untuk tindakan kriminal seperti pencurian identitas, akses tidak sah ke akun, dan penipuan finansial [2].

Di era digital yang semakin kompleks, serangan phishing telah menjadi salah satu ancaman utama tidak hanya bagi individu, tetapi juga bagi institusi skala besar, termasuk sektor pendidikan tinggi. Perguruan tinggi, khususnya yang telah mengadopsi sistem akademik berbasis daring, menyimpan data sensitif yang sangat bernilai, seperti biodata mahasiswa, informasi akademik dosen, dan data keuangan institusi. Berdasarkan hasil studi oleh sistem informasi akademik menjadi salah satu target utama serangan siber karena kurangnya penerapan mekanisme keamanan yang memadai, serta rendahnya literasi keamanan siber di kalangan pengguna sistem [3].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

Selain kelemahan pada sisi autentikasi, terdapat pula faktor lain yang meningkatkan risiko terhadap sistem ini, yaitu pemanfaatan layanan tunneling seperti Ngrok. Ngrok merupakan alat yang memungkinkan expose server lokal ke jaringan publik melalui jaringan tunneling. Dalam konteks simulasi serangan siber, Ngrok sering digunakan oleh peneliti atau pihak tidak bertanggung jawab untuk membuat situs phishing yang dapat diakses publik, meskipun dijalankan dari komputer lokal [4]. Jika dipadukan dengan tools seperti Kali Linux dan Social Engineering Toolkit (SET), pelaku dapat dengan mudah merekayasa halaman login palsu dan menyebarkannya ke target sasaran.

Beberapa studi sebelumnya telah mengangkat topik serupa, yaitu mengenai simulasi serangan phishing menggunakan berbagai tools open-source seperti Kali Linux dan SET [5] [6]. Studi-studi ini seringkali mendemonstrasikan efektivitas teknik social engineering dalam memperoleh kredensial secara real-time, menyoroti bagaimana alat tersebut mampu menangkap data setelah input dari korban [7], [8], [9]. Pendekatan etis dalam simulasi serangan siber, yang menekankan penggunaan lingkungan terkontrol dan akun dummy, juga telah menjadi rekomendasi penting dalam riset keamanan untuk menjaga aspek etika dan kepatuhan hukum [10]. Namun, sebagian besar penelitian tersebut tidak secara khusus menyoroti sistem informasi akademik berbasis cloud yang digunakan oleh institusi pendidikan tinggi.

Penelitian terkait juga menunjukkan pentingnya sistem pendeteksi link tidak sah, karena situs yang tidak mengenali sumber link eksternal sangat rawan dieksploitasi melalui teknik tunneling [11], [12]. Selain itu, ancaman phishing tidak hanya terbatas pada email atau website, tetapi juga meluas ke platform seperti aplikasi pesan instan, yang memerlukan analisis ancaman yang komprehensif [13]. Kurangnya monitoring perilaku login dan rendahnya kesadaran keamanan siber di kalangan pengguna sistem juga menjadi faktor kerentanan yang signifikan, sebagaimana ditekankan oleh studi yang berfokus pada peningkatan kesadaran keamanan siber dan implementasi keamanan berbasis kecerdasan buatan untuk mengatasi phishing [14][15].

Maka dari itu, terdapat gap penelitian yang signifikan, yakni kurangnya analisis teknis dan empiris terkait potensi kerentanan pada sistem akademik yang belum menerapkan protokol keamanan berlapis, serta integrasi pemahaman mendalam tentang social engineering dan peran tools simulasi dalam mengidentifikasi celah ini secara spesifik pada lingkungan perguruan tinggi.

Penelitian ini bertujuan untuk menganalisis potensi kerentanan situs sttsundermann.siakadcloud.com terhadap serangan phishing, dengan menggunakan simulasi teknis berbasis Kali Linux, Ngrok, dan Social Engineering Toolkit (SET). Simulasi dilakukan dalam lingkungan yang terkendali, tanpa melibatkan pengguna aktual sebagai korban, untuk menjaga aspek etika penelitian. Proses simulasi mencakup tahapan pembuatan situs tiruan, penyebaran tautan phishing melalui skenario sosial, serta pengumpulan data login sebagai indikator efektivitas serangan.

Secara teoretis, penelitian ini diharapkan dapat memperkaya literatur dalam bidang keamanan siber, khususnya pada subbidang social engineering attack dan keamanan sistem informasi pendidikan. Analisis ini juga diharapkan dapat membantu mengidentifikasi pola kerentanan umum yang sering tidak disadari oleh pengembang maupun administrator sistem akademik. Di sisi lain, secara praktis, hasil temuan dari simulasi ini diharapkan menjadi acuan bagi institusi pendidikan tinggi dalam membangun kebijakan keamanan yang lebih ketat dan menyeluruh, termasuk penerapan teknologi autentikasi ganda dan sistem verifikasi halaman situs web.

Selain itu, urgensi penerapan standar keamanan global seperti ISO/IEC 27001 dan kerangka kerja NIST Cybersecurity Framework juga menjadi sorotan penting dalam penelitian ini. Standar tersebut dapat menjadi pedoman dalam merancang sistem keamanan digital yang adaptif, terstruktur, dan berbasis risiko. Tidak hanya itu, peningkatan literasi digital bagi sivitas akademika dan kolaborasi lintas sektor dengan praktisi keamanan siber juga menjadi kunci dalam memperkuat daya tahan institusi terhadap serangan yang semakin canggih dan terorganisir.

Dengan pendekatan yang komprehensif ini, diharapkan hasil penelitian dapat memberikan dampak nyata dalam meningkatkan kesadaran keamanan digital dan mendorong terciptanya ekosistem akademik yang lebih aman dari ancaman phishing.

2. METODOLOGI 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 kerentanan terhadap serangan phishing pada sistem informasi akademik sttsundermann.siakadcloud.com. Simulasi dilakukan dalam lingkungan virtual terkendali, tanpa melibatkan data pengguna asli, untuk menjaga etika dan keamanan selama penelitian.

Sesuai dengan [16] pendekatan eksperimen sangat cocok dalam konteks keamanan siber karena memungkinkan peneliti untuk menguji skenario ancaman nyata dalam kondisi terkontrol. Pendekatan ini menghasilkan data observasi kuantitatif yang valid untuk dianalisis secara sistematis.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

2.2. Target, Etika dan Validitas Simulasi

Penelitian ini menggunakan target dummy (akun simulasi internal) sebagai objek uji coba. Tidak ada data pengguna asli yang digunakan. Simulasi dilakukan pada sistem virtual (VirtualBox) dengan konfigurasi khusus untuk mendokumentasikan interaksi antara halaman phishing dan sistem terminal.

Untuk menjaga validitas hasil, simulasi dilakukan sebanyak lima sesi pengujian terpisah, dengan konfigurasi serupa untuk setiap sesi. Reliabilitas diuji dengan pengulangan skenario dan pencatatan hasil otomatis di terminal Kali Linux. Data login yang masuk tercatat secara real-time, dengan format dan waktu tangkap yang dikonfirmasi konsisten di setiap sesi.

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:

- 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, salah satunya adalah
- Social Engineering Toolkit (SET). Social Engineering Toolkit (SET): Digunakan untuk menggandakan halaman login situs target melalui fitur Credential Harvester Attack. Alat ini mampu meniru tampilan situs asli dengan akurasi visual tinggi, sehingga dapat menipu target dengan efektif.
- Ngrok: Layanan reverse proxy yang digunakan untuk mengekspos server lokal ke jaringan publik, menghasilkan URL HTTPS sementara yang tampak sah di mata target.
- Laptop/PC: Dengan spesifikasi mendukung virtualisasi atau dual-boot Kali Linux.
- Akun Ngrok aktif dan koneksi internet stabil: Diperlukan untuk menghubungkan server lokal ke jaringan luar.

2.4 Langkah-langkah Simulasi

Simulasi serangan phishing dilakukan dalam beberapa tahapan sistematis menggunakan sistem operasi Kali Linux, *Social Engineering Toolkit* (SET), dan layanan tunneling Ngrok. Setiap langkah dilakukan dalam lingkungan virtual yang terkendali, dengan target dummy untuk menjamin aspek etis. Berikut ini adalah ringkasan tahapan yang dilakukan dalam proses simulasi:

Tabel 1. Langkah-langkah Simulasi

NO	TAHAPAN	PENEJELASAN
1	Konfigurasi akun dan authtoken	Autentikasi Ngrok untuk memulai koneksi aman.
2	Jalankan SET di Kali Linux	Memilih menu Website Attack Vector → Credential Harvester.
3	Kloning halaman login target	Kloning situs https://sttsundermann.siakadcloud.com/gate/login
4	Ekspos halaman menggunakan Ngrok	Mendapatkan URL publik HTTPS dari terminal.
5	Simulasi akses dan pencatatan	Login dummy dilakukan, dan data ditangkap otomatis di terminal SET.

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 login dummy melalui terminal Kali Linux.

Gambar 1 Diagram Alur Simulasi Serangan Phishing

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

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 dalam konteks peningkatan keamanan sistem informasi akademik.

2.6 Parameter Pengujian

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

Tabel 2. Parameter Pengujian dalam Simulasi Phishing

Parameter	Indikator Pengukuran
Jumlah tautan yang dibuka	Mengukur berapa banyak URL phishing yang berhasil dibuka oleh target simulasi
Kredensial yang tertangkap	Jumlah data login (username dan password) yang berhasil direkam oleh SET Toolkit
Waktu tangkap	Selisih waktu antara input data oleh target dan data muncul di terminal Kali Linux
Konsistensi antar sesi	Mengukur apakah hasil pada tiap sesi uji cenderung stabil atau bervariasi secara signifikan

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 Hasil Simulasi dan Serangan Phishing

Simulasi serangan phishing pada website sttsundermann.siakadcloud.com dilakukan dalam lima sesi terpisah menggunakan kombinasi Kali Linux, *Social Engineering* Toolkit (SET), dan Ngrok. Seluruh proses simulasi menggunakan akun dummy untuk menjaga aspek etika dan kepatuhan hukum. Parameter yang diukur pada setiap sesi meliputi status akses tautan, keberhasilan penangkapan kredensial, dan waktu tangkap data. Hasil rinci dari kelima sesi disajikan dalam Tabel 3.

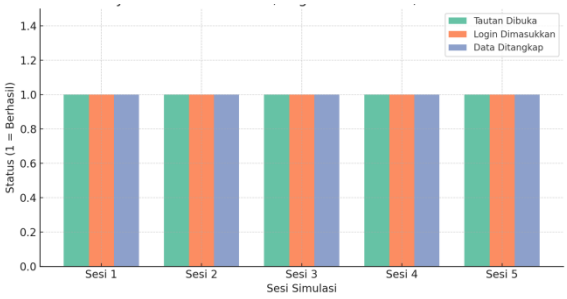
Tabel 3. Hasil Simulasi Serangan Phishing (5 sesi uji)

Sesi	Tautan Dibuka	Login Dimasukkan	Data Tertangkap	Waktu Tangkap (detik)
1	Ya	Ya	Ya	2,5
2	Ya	Ya	Ya	2,3
3	Ya	Ya	Ya	2,6
4	Ya	Ya	Ya	2,4
5	Ya	Ya	Ya	2,5
Rata-rata				**2,46**

Berdasarkan data kuantitatif yang tersaji dalam Tabel 3, dapat diobservasi bahwa seluruh lima sesi simulasi (session 1 hingga session 5) menunjukkan tingkat keberhasilan yang sempurna atau 100% dalam merekam kredensial target. Ini berarti setiap kali tautan phishing berhasil diakses dan login data dimasukkan ke halaman tiruan, informasi tersebut selalu berhasil ditangkap oleh sistem penyerang. Aspek lain yang sangat krusial adalah rata-rata waktu tangkap data, yang tercatat sangat cepat, yaitu hanya 2,46 detik. Kecepatan ini bukan sekadar angka statistik; ia membuktikan betapa rentannya pengguna terhadap serangan phishing yang dirancang dengan baik, di mana pelaku dapat mengeksploitasi kecepatan respons atau kurangnya kehati-hatian pengguna saat mencoba login ke suatu sistem. Dalam skenario nyata, kecepatan seperti ini nyaris tidak memberikan peluang bagi korban untuk menyadari atau membatalkan tindakan mereka secara manual, yang berujung pada potensi kebocoran data yang masif dalam waktu singkat. Tingkat keberhasilan yang konsisten ini juga menegaskan bahwa serangan berbasis rekayasa sosial, bahkan dengan alat open-source yang sederhana, dapat menjadi ancaman yang sangat efektif dan sulit dideteksi oleh individu tanpa literasi keamanan siber yang memadai.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

Visualisasi dari beberapa tahapan dan hasil simulasi disajikan dalam gambar-gambar berikut untuk memberikan pemahaman yang lebih konkret:

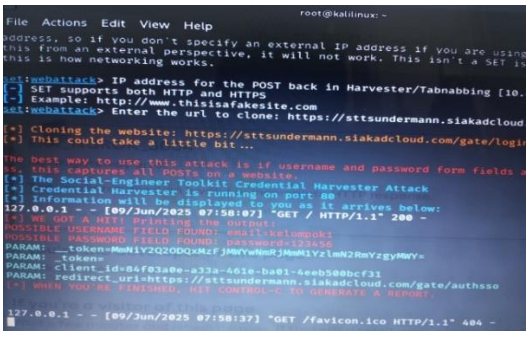


gambar 2.Grafik Keberhasilan Akses dan Penangkapan Data

Grafik ini secara visual merepresentasikan konsistensi tinggi dalam keberhasilan akses tautan dan penangkapan kredensial di setiap sesi simulasi. Bentuk grafik yang menunjukkan garis lurus atau batangan yang seragam pada tingkat keberhasilan 100% menegaskan potensi ancaman serius dan risiko inheren terhadap sistem akademik yang diuji. Ini menunjukkan bahwa metode serangan yang digunakan memiliki tingkat efektivitas yang sangat tinggi dan dapat diandalkan oleh penyerang untuk mencapai tujuannya.

gambar 3. Halaman Login STTSunderman yang Terkloning

Gambar diatas menampilkan screenshot dari halaman login tiruan yang berhasil direplikasi secara persis menggunakan Social Engineering Toolkit (SET). Antarmuka halaman palsu ini didesain agar semirip mungkin dengan tampilan situs asli https://sttsundermann.siakadcloud.com/gate/login, mencakup logo, skema warna, tata letak, dan elemen visual lainnya. Tingkat kemiripan yang tinggi ini menjadi faktor krusial dalam menipu target, membuat mereka percaya bahwa mereka sedang berinteraksi dengan halaman login yang sah. Visualisasi ini menegaskan betapa mudahnya penyerang membuat kloning situs yang meyakinkan untuk tujuan jahat.



gambar 4. Penangkapan Kredensial di Terminal Kali Linux

Pada gambar diatas menunjukkan tampilan terminal Kali Linux pada saat kredensial (username dan password) yang dimasukkan oleh target pada halaman phishing palsu berhasil tertangkap dan ditampilkan secara real-time. Tampilan output pada terminal ini mengonfirmasi bahwa data sensitif telah berhasil disadap dan terekam pada sistem penyerang. Ini adalah bukti konkret dari efektivitas metode penyadapan data yang diterapkan dalam simulasi, menunjukkan bahwa informasi penting dapat dengan cepat berpindah tangan dari korban ke pelaku serangan.

3.2 Identifikasi Kerentanan Sistem Target

Hasil simulasi ini secara jelas mengidentifikasi beberapa kerentanan signifikan pada situs https://sttsundermann.siakadcloud.com/gate/login yang membuatnya sangat rentan terhadap serangan phishing berbasis social engineering. Kerentanan ini bukan hanya bersifat teoritis, melainkan telah dibuktikan secara empiris melalui keberhasilan simulasi penangkapan kredensial:

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

1. Ketiadaan Mekanisme Autentikasi Tambahan: Salah satu kerentanan paling mendasar yang teridentifikasi adalah tidak adanya implementasi *Two-Factor Authentication (*2FA) atau CAPTCHA pada halaman login sistem. Ketiadaan 2FA berarti bahwa jika kredensial (username dan password) pengguna berhasil dicuri melalui phishing, penyerang akan memiliki akses penuh ke akun tersebut tanpa memerlukan verifikasi tambahan. Ini menciptakan "titik kegagalan tunggal" yang sangat berbahaya. Tanpa 2FA, lapisan keamanan sekunder yang seharusnya melindungi akun menjadi tidak ada, memungkinkan penyerang untuk masuk dengan mudah. Selain itu, ketiadaan CAPTCHA juga merupakan celah signifikan. CAPTCHA berfungsi sebagai penghalang untuk mencegah serangan brute-force otomatis atau spamming tautan phishing secara massal oleh bot. Tanpa CAPTCHA, penyerang dapat menggunakan script otomatis untuk mencoba berbagai kombinasi kredensial atau menyebarkan link secara luas tanpa hambatan, meningkatkan skala potensi serangan.
2. Rentannya Penggunaan Layanan Tunneling (Ngrok): Layanan Ngrok, meskipun dirancang untuk tujuan pengembangan dan pengujian dengan memungkinkan server lokal di-expose ke internet publik melalui URL HTTPS, sangat rentan disalahgunakan dalam konteks serangan phishing. Dalam simulasi ini, Ngrok digunakan untuk menyajikan halaman phishing yang berhasil dikloning ke jaringan internet. Dengan demikian, link yang dihasilkan Ngrok terlihat sah karena menggunakan protokol HTTPS dan seringkali memiliki domain yang tampak generik dan tidak mencurigakan bagi pengguna awam. Sistem atau pengguna yang tidak memiliki mekanisme validasi URL atau deteksi anomali pada link eksternal sangat mudah tertipu oleh URL yang dihasilkan Ngrok ini. Kemampuan Ngrok untuk menyembunyikan alamat IP asli penyerang juga mempersulit pelacakan dan mitigasi serangan.
3. Kemudahan Replika Halaman Login: *Social Engineering Toolkit* (SET) terbukti sebagai alat yang sangat ampuh dalam mereplikasi halaman login asli dari https://sttsundermann.siakadcloud.com/gate/login dengan tingkat presisi visual yang sangat tinggi. SET mampu mengkloning seluruh elemen desain, termasuk logo, skema warna, tata letak, dan elemen interaktif, sehingga menciptakan halaman tiruan yang nyaris identik dengan aslinya. Tingkat kemiripan visual yang luar biasa ini merupakan faktor kunci keberhasilan serangan karena secara efektif menipu mata pengguna. Pengguna awam, yang seringkali hanya melihat tampilan luar, akan kesulitan membedakan antara situs asli dan situs palsu. Hal ini menunjukkan bahwa sistem yang bergantung pada pengenalan visual pengguna untuk keamanan sangat rentan terhadap teknik kloning semacam ini, yang semakin memperkuat efektivitas serangan rekayasa sosial.
4. Kurangnya Kesadaran Keamanan Pengguna: Tingkat keberhasilan 100% dalam penangkapan data kredensial pada setiap sesi simulasi secara empiris menunjukkan bahwa tingkat kesadaran keamanan siber di kalangan pengguna (dalam skenario dummy) masih sangat rendah. Umumnya, pengguna cenderung tidak memeriksa detail penting seperti URL lengkap (apakah ada perbedaan domain atau sub-domain yang mencurigakan), validitas sertifikat SSL (apakah sertifikat dikeluarkan untuk domain yang benar), atau indikator keamanan lainnya sebelum dengan cepat memasukkan kredensial pribadi mereka. Kurangnya kehati-hatian ini menjadi celah terbesar yang dieksploitasi oleh pelaku phishing. Edukasi dan pelatihan berkelanjutan mengenai ancaman phishing dan cara mengidentifikasinya adalah fundamental untuk membangun garis pertahanan pertama yang kuat di tingkat pengguna.

3.3 Implikasi Keamanan dan Rekomendasi Mitigasi

Temuan penelitian ini memiliki implikasi yang serius dan mendalam terhadap keamanan data di lingkungan pendidikan tinggi, khususnya pada sistem informasi akademik. Keberhasilan simulasi serangan phishing menekankan urgensi implementasi langkah-langkah mitigasi yang proaktif dan berlapis untuk melindungi aset informasi yang berharga:

1. Risiko Pencurian Data Akademik dan Pribadi: Keberhasilan penangkapan kredensial login berarti bahwa data-data krusial seperti biodata mahasiswa, informasi akademik (nilai, riwayat studi), data keuangan dosen, dan informasi sensitif lainnya yang tersimpan dalam sistem informasi akademik https://sttsundermann.siakadcloud.com/gate/login sangat rentan untuk dicuri. Data-data ini dapat disalahgunakan secara luas, mulai dari manipulasi nilai akademis, pencurian identitas untuk pembukaan rekening atau pinjaman ilegal, hingga penipuan finansial yang merugikan individu dan institusi.
2. Kerugian Reputasi Institusi dan Kepercayaan Pengguna: Insiden kebocoran data berskala besar atau serangan phishing yang sukses dapat merusak reputasi institusi secara signifikan. Kepercayaan dari mahasiswa, orang tua, calon mahasiswa, dan mitra kerja dapat menurun drastis, berpotensi memengaruhi jumlah pendaftar baru atau kerja sama strategis di masa mendatang. Membangun kembali kepercayaan yang telah rusak adalah proses yang panjang dan sulit, yang seringkali memakan sumber daya besar.
3. Potensi Tindak Kriminal Lanjutan dan Serangan Lebih Kompleks: Kredensial login yang berhasil diperoleh oleh penyerang bukan hanya akhir dari serangan, tetapi seringkali menjadi pintu masuk awal (initial access) untuk melancarkan serangan siber yang jauh lebih kompleks dan merusak. Penyerang dapat menggunakan akses ini untuk menyuntikkan malware (misalnya ransomware), melakukan pencurian data dalam skala yang lebih besar dari basis data internal, mengganggu operasional sistem (denial of service), atau bahkan memanipulasi informasi kritis dalam sistem akademik. Hal ini dapat berujung pada kerugian finansial yang sangat besar dan disrupsi layanan yang parah.

Untuk memitigasi kerentanan yang teridentifikasi dan mencegah konsekuensi serius di atas, beberapa rekomendasi strategis dan teknis yang dapat diimplementasikan oleh institusi adalah sebagai berikut:

1. Implementasi Autentikasi Multifaktor (MFA): Institusi harus segera menerapkan MFA sebagai standar untuk setiap proses login. MFA menambahkan lapisan verifikasi keamanan kedua, seperti kode OTP yang dikirim ke ponsel, sidik

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

jari, atau token perangkat keras. Dengan MFA, bahkan jika penyerang berhasil mencuri username dan password, mereka tidak akan bisa mengakses akun tanpa verifikasi kedua dari pengguna yang sah. Ini secara drastis mengurangi risiko akses tidak sah bahkan ketika kredensial utama telah disusupi.

2. Penerapan CAPTCHA atau Sistem Pendeteksi Bot: Mengintegrasikan CAPTCHA yang kuat pada halaman login atau sistem pendaftaran dapat secara efektif mencegah upaya brute-force otomatis dan serangan spamming tautan phishing yang dilakukan oleh bot. Selain itu, penggunaan solusi keamanan yang lebih canggih seperti sistem deteksi bot dapat mengidentifikasi dan memblokir lalu lintas otomatis yang mencurigakan sebelum mencapai halaman login.
3. Sistem Pendeteksi Anomali Login: Menerapkan sistem berbasis machine learning atau Artificial Intelligence (AI) yang secara terus-menerus memantau pola login pengguna. Sistem ini dapat mendeteksi perilaku login yang tidak biasa, seperti akses dari lokasi geografis yang tidak dikenal, upaya login yang gagal berulang kali dalam waktu singkat, atau login pada jam-jam yang tidak wajar. Jika anomali terdeteksi, sistem dapat memblokir akses secara otomatis atau memicu verifikasi tambahan, sehingga mencegah akses tidak sah.
4. Edukasi dan Pelatihan Kesadaran Keamanan Siber Berkelanjutan: Kampanye edukasi dan pelatihan yang komprehensif serta berkelanjutan harus menjadi prioritas bagi seluruh sivitas akademika (mahasiswa, dosen, staf administrasi). Pelatihan ini harus mencakup materi tentang cara mengenali ciri-ciri serangan phishing (misalnya, memeriksa URL secara cermat, mengidentifikasi kesalahan tata bahasa atau desain pada situs web), pentingnya memverifikasi sertifikat SSL, tidak mengklik tautan yang mencurigakan, dan praktik terbaik dalam mengelola kata sandi yang kuat dan unik. Simulasi phishing internal yang dilakukan secara berkala dapat menjadi cara efektif untuk melatih dan menguji kesiapan pengguna.
5. Implementasi Kebijakan Keamanan Jaringan dan Sistem Deteksi Intrusi (IDS): Institusi perlu menerapkan kebijakan keamanan jaringan yang ketat untuk memblokir akses ke domain-domain yang dikenal sebagai sumber phishing atau penyedia layanan tunneling yang sering disalahgunakan (seperti Ngrok jika tidak diperlukan). Selain itu, penyebaran Sistem Deteksi Intrusi (IDS) dapat membantu memantau lalu lintas jaringan untuk mengidentifikasi pola serangan atau anomali yang mengindikasikan upaya phishing atau intrusi.
6. Mendorong Verifikasi Eksternal Link: Selain edukasi, institusi dapat menyediakan atau mendorong penggunaan tools bantu yang memungkinkan pengguna untuk memverifikasi keaslian suatu tautan sebelum mengkliknya. Ini bisa berupa ekstensi browser keamanan atau layanan online yang dapat menganalifikasi URL.

Aspek Etika dan Hukum Peneltian

Penelitian ini dilaksanakan dengan pendekatan etis dan legal, hanya menggunakan akun dummy, dan tidak melibatkan data pengguna aktual. Halaman phishing tidak dibagikan ke luar atau digunakan untuk tujuan lain selain penelitian. Dalam konteks hukum Indonesia, tindakan pembuatan halaman palsu dan pengumpulan data tanpa izin melanggar UU ITE (No. 11 Tahun 2008) serta UU Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022. Oleh karena itu, simulasi seperti ini harus dilakukan secara terkendali dan hanya untuk kepentingan ilmiah atau evaluasi sistem keamanan.

4 KESIMPULAN

Penelitian ini secara empiris menunjukkan kerentanan situs akademik sttsundermann.siakadcloud.com terhadap serangan phishing menggunakan Kali Linux, Ngrok, dan Social Engineering Toolkit (SET). Dari lima sesi simulasi yang dilakukan dalam lingkungan terkendali dengan akun dummy, 100% kredensial berhasil ditangkap dengan rata-rata waktu tangkap sangat cepat, yaitu 2,46 detik. Keberhasilan ini menyoroti tiga kerentanan utama: ketiadaan Autentikasi Multifaktor (MFA) dan CAPTCHA, kemudahan penyalahgunaan layanan Ngrok untuk membuat tautan phishing yang tampak sah, serta tingginya presisi replikasi halaman login oleh SET. Implikasinya sangat serius, mencakup risiko pencurian data akademik dan pribadi, kerugian reputasi institusi, dan potensi serangan siber lanjutan. Untuk mitigasi, direkomendasikan implementasi MFA, CAPTCHA atau sistem pendeteksi bot, sistem pendeteksi anomali login berbasis AI, serta edukasi keamanan siber berkelanjutan bagi seluruh sivitas akademika. Selain itu, kebijakan keamanan jaringan yang ketat dan penggunaan Sistem Deteksi Intrusi (IDS) juga penting. Penelitian ini menekankan urgensi peningkatan kesadaran dan penguatan sistem keamanan digital di perguruan tinggi untuk menghadapi ancaman phishing yang semakin canggih.

REFERENCES

[1] Y. Purwanti, F. Rachman, T. Gunawan, and A. Kartadinata, "Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung," *Audi AP J. Penelit. Huk.*, vol. 2, no. 01, pp. 64–71, 2023, doi: 10.24967/jaeap.v2i01.2088.

[2] B. Benyamin, P. Studi, S. Ilmu, F. Hukum, and U. Hasanuddin, "Analisis Yuridis Tindak Pidana Cyber Crime Indonesia Juridical Analysis of the Criminal Offense of Cyber Crime Phishing in the Provisions of Indonesian Positive Law," 2024.

[3] G. Wijaya, T. Tan, S. E. Prasetyo, and S. Pho, "Analisis Perbandingan VPN Tunnel antara ngrok Edge Cloud vs Public IP Address menggunakan Open VPN," vol. 4, no. 1, pp. 378–391, 2024.

[4] K. Ruswandi, M. R. Z. Pohan, K. V. Halim, and S. N. Neyman, "Strategi Pencegahan Efektif terhadap Serangan DDoS Slowloris menggunakan Kali Linux dan Linux Mint," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2645.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 390-397
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.398

[5] B. Gumay, A. H. Hendrawan, F. Satrya, F. Kusumah, T. Informatika, and U. I. Khaldun, "ISSN : 2460-1861 (Print), 2615-4250 (Online)," vol. 10, no. 2, pp. 297–305, 2024.

[6] F. D. Silalahi, "Keamanan Cyber (Cyber Security)," *Penerbit Yayasan Prima Agus Tek.*, pp. 1–285, 2022, [Online]. Available: http://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/367

[7] H. S. Harahap, A. A. Rahman, I. Suraswati, and S. N. Neyman, "Memahami Cara Kerja Phishing menggunakan Tools pada Kali Linux," *J. Internet Softw. Eng.*, vol. 1, no. 2, pp. 1–11, 2024.

[8] T. F. Ramadhan, I. Ramadhan, and A. A. Pangestu, "Analisis Keamanan Teknologi Dalam Menghadapi Ancaman Phising," no. 55.

[9] G. Aparna, B. V. Krishna, C. K. Reddy, K. Latha, and M. Akshitha, "Phishing simulations," no. March, 2025.

[10] D. Anjheli, "Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 , lebih dari 215 juta penduduk telah terhubung," vol. 4, no. 1, 2024.

[11] A. D. Harahap, D. Juardi, and A. S. Y. Irawan, "Rancang Bangun Sistem Pendeteksi Link Phishing Menggunakan Algoritma Random Forest Berbasis Web," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 3, 2024, doi: 10.23960/jitet.v12i3.4858.

[12] J. Gusti, A. Ginting, B. Arifwidodo, and E. Wahyudi, "Virtual Privat Network : Koneksi Keamanan pada Aplikasi Berbasis Android Virtual Private Network : Security Connection in Android Based Applications," vol. 8275, pp. 32–41, 2025.

[13] M. W. A. Prastya, M. Tahir, A. A. Ningrum, and A. P. Zaibintoro, "Analisis Ancaman Pishing melalui Aplikasi WhatsApp : Review Metode Studi Analisis Ancaman Pishing melalui Aplikasi WhatsApp : Review Metode Studi Literatur," no. May, 2024, doi: 10.32672/jnkti.v7i3.7551.

[14] B. Wibowo and T. Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *J. Pengabdi. Masy. Sultan Indones.*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.58291/abdisultan.v2i1.294.

[15] U. A. Pringsewu, "Volume 7 Issue 1 Aisyah Journal of Informatics and Electrical Engineering IMPLEMENTASI SISTEM KEAMANAN SIBER BERBASIS ARTIFICIAL INTELLIGENCE UNTUK MENGATASI SERANGAN PHISHING Aisyah Journal of Informatics and Electrical Engineering Aisyah Journal of Info," vol. 7, no. 1, pp. 94–98.

[16] D. Iriyadi, "Telaah Kritis Metode-Metode Dalam Penelitian Ilmiah," vol. 1, pp. 22–28, 2024.