JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

Simulasi Teknik Phishing terhadap Situs Tiruan Facebook dan SIAKAD UNIRAYA Menggunakan Zphisher dan Ngrok

Boy Setyawan Zalukhu[1], Fredin Samohouni Zai[1], Elena Dementieva Lase[1], Rosania Waruwu[1], Markus Prayoga Telaumbanua[1], Ofelius Laia[1,*]

[1]Fakultas Sains dan Teknologi, Program Studi Teknologi Informasi, Universitas Nias, Kota Gunungsitoli, Indonesia
Email: [1]setyawanboy680@gmail.com, [2]fredinsamohounizai@gmail.com, [3]elenalase3@gmail.com, [4]rosaniawaruwu2@gmail.com, [5]yogatelaumbanua28@gmail.com, [6]ofeliuslaia@gmail.com
(* Email Corresponding Author: ofeliuslaia@gmail.com)
Received: 18 Juni 2025 | Revision: 20 Juni 2025 | Accepted: 23 Juni 2025

Abstrak

Penelitian ini bertujuan untuk mensimulasikan serangan phishing menggunakan dua alat populer, yaitu Zphisher dan Ngrok, dalam konteks edukatif. Simulasi dilakukan melalui pembuatan situs tiruan dari Facebook dan Sistem Informasi Akademik Universitas Raya (SIAKAD UNIRAYA), kemudian diuji untuk menangkap data login fiktif. Zphisher digunakan untuk menghasilkan situs phishing berbasis template secara otomatis, sedangkan Ngrok dikombinasikan dengan Social-Engineer Toolkit (SET) untuk membangun halaman phishing yang lebih fleksibel dan dapat dikustomisasi. Hasil eksperimen menunjukkan bahwa kedua alat mampu meniru tampilan situs asli secara efektif dan berhasil menangkap informasi penting seperti alamat IP, nama pengguna (username), dan kata sandi (password). Dari sisi penggunaan, Zphisher lebih unggul dalam kemudahan dan kecepatan implementasi, sementara Ngrok memberikan tingkat kontrol dan keamanan lebih tinggi dalam pengujian tertutup. Seluruh proses dilakukan di lingkungan terbatas dan tidak menyebarkan tautan secara publik, serta tidak menggunakan data asli untuk menjaga etika penelitian. Penelitian ini memberikan wawasan praktis dalam mengenali teknik phishing serta menekankan pentingnya menjaga keamanan data pribadi di era digital saat ini.

Kata Kunci: Phishing, Zphisher, Ngrok, Keamanan Digital, Rekayasa Sosial

Abstract

This research aims to simulate phishing attacks using two popular tools, Zphisher and Ngrok, in an educational context. The simulation was conducted by creating mock sites from Facebook and Universitas Raya Academic Information System (SIAKAD UNIRAYA), then tested to capture fictitious login data. Zphisher was used to automatically create template-based phishing sites, while Ngrok was combined with Social-Engineer Toolkit (SET) to create more flexible and customizable phishing pages. Experimental results show that both tools are able to effectively mimic the appearance of the original site and successfully capture important information such as IP addresses, usernames, and passwords. In terms of usability, Zphisher was superior in terms of ease and speed of implementation, while Ngrok provided a higher level of control and security in closed tests. The entire process was conducted in a restricted environment and did not share links publicly, and did not use real data to maintain research ethics. This research provides practical insights to recognize phishing techniques and emphasizes the importance of keeping personal data safe in today's digital age.

Keywords: *Phishing, Zphisher, Ngrok, Digital Security, Social Engineering*

1. PENDAHULUAN

Keamanan siber telah menjadi perhatian utama di era digital saat ini. Ancaman siber terus berkembang, dengan teknik serangan yang semakin canggih dan beragam. Salah satu ancaman yang paling umum dan efektif adalah phishing [1]. Phishing merupakan upaya penipuan untuk mendapatkan informasi sensitif seperti username, password, atau informasi keuangan, dengan menyamar sebagai entitas terpercaya dalam komunikasi elektronik [2]. Serangan phishing sering kali memanfaatkan teknik rekayasa sosial untuk memanipulasi korban agar mengungkapkan informasi pribadi mereka. Teknik ini menyasar berbagai kalangan, mulai dari individu biasa hingga institusi besar, karena efektivitasnya dalam mengecoh pengguna yang kurang waspada. Di tengah maraknya digitalisasi, kesadaran terhadap keamanan informasi menjadi hal yang sangat penting, terlebih ketika semakin banyak aktivitas dilakukan secara daring.

Data menunjukkan bahwa serangan phishing terus meningkat secara global, menyebabkan kerugian finansial yang signifikan dan merusak reputasi organisasi [3]. Banyak organisasi dan perusahaan harus menanggung biaya besar untuk pemulihan sistem, memperbaiki kredibilitas, dan memberikan kompensasi kepada pelanggan yang terdampak. Di Indonesia, kasus phishing juga menjadi masalah serius, dengan jumlah laporan yang meningkat setiap tahunnya. Hal ini dipengaruhi oleh berbagai faktor, termasuk rendahnya kesadaran masyarakat terhadap keamanan siber serta mudahnya akses terhadap alat-alat phishing [4]. Selain itu, banyak pengguna internet masih belum memahami bagaimana membedakan tautan atau situs palsu dengan yang asli, sehingga risiko menjadi korban semakin tinggi. Kemudahan mendapatkan perangkat lunak seperti pembuat situs palsu dan layanan tunneling semakin memperbesar peluang pelaku dalam melakukan aksinya.

Penelitian ini dilatarbelakangi oleh meningkatnya ancaman phishing yang menargetkan pengguna internet di Indonesia, khususnya pada platform media sosial seperti Facebook dan sistem informasi akademik (SIAKAD)

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

perguruan tinggi. Platform-platform tersebut menyimpan data pribadi yang bernilai tinggi, sehingga menjadi sasaran utama bagi pelaku kejahatan siber [5]. Facebook merupakan media sosial yang digunakan secara luas, sehingga memiliki banyak celah bagi pelaku untuk menyamar dan menjebak korban. Sementara itu, SIAKAD menyimpan data akademik dan pribadi mahasiswa seperti nama lengkap, NIM, nilai, hingga riwayat pembayaran. Data-data ini, jika berhasil dicuri, dapat dimanfaatkan untuk tujuan yang merugikan, seperti penyebaran informasi palsu atau penipuan yang lebih kompleks. Oleh karena itu, pemahaman mengenai metode serangan menjadi langkah awal yang penting dalam upaya mitigasi.

Tujuan dari penelitian ini adalah untuk mensimulasikan teknik phishing yang menggunakan alat Zphisher dan Ngrok pada situs tiruan Facebook dan SIAKAD UNIRAYA. Penelitian ini bertujuan untuk mengidentifikasi bagaimana teknik phishing dapat dilakukan, menganalisis potensi risiko yang ditimbulkan, serta memberikan edukasi mengenai cara mendeteksi dan mencegah serangan phishing. Dengan memahami cara kerja serangan, pengguna maupun pengelola sistem dapat lebih waspada dalam menghadapi ancaman dan merancang langkah-langkah perlindungan yang lebih tepat. Simulasi yang dilakukan dalam penelitian ini juga bertujuan untuk menguji efektivitas masing-masing alat dalam menciptakan halaman phishing serta kemampuannya dalam menangkap informasi sensitif secara fiktif.

Kontribusi dari penelitian ini adalah memberikan gambaran praktis tentang bagaimana serangan phishing dilakukan menggunakan alat-alat yang relatif mudah diakses. Selain itu, penelitian ini juga memberikan analisis risiko secara spesifik terhadap platform Facebook dan SIAKAD UNIRAYA, serta memberikan rekomendasi mitigasi yang dapat diterapkan untuk meningkatkan keamanannya. Penelitian ini tidak hanya bertujuan untuk mengungkapkan celah keamanan, tetapi juga untuk memberikan edukasi kepada pengguna dan pengelola sistem agar lebih bijak dan tanggap dalam menghadapi upaya penipuan digital. Hasil yang diperoleh dari simulasi ini dapat dijadikan sebagai bahan pertimbangan dalam meningkatkan sistem keamanan, baik dari sisi teknis maupun dari sisi kesadaran pengguna.

Penggunaan Zphisher dan Ngrok dalam simulasi ini dipilih karena kemudahan penggunaannya serta ketersediaannya secara luas, sehingga memudahkan peneliti untuk melakukan simulasi dan memberikan gambaran yang jelas tentang bagaimana serangan phishing dapat dilakukan oleh pelaku. Zphisher memungkinkan pembuatan situs phishing secara cepat dan otomatis dengan berbagai pilihan template yang menyerupai situs asli. Sementara itu, Ngrok memberikan layanan tunneling yang memungkinkan halaman phishing diakses secara publik, meskipun dijalankan secara lokal. Kedua alat ini merepresentasikan kombinasi yang umum digunakan dalam skenario phishing oleh pelaku kejahatan siber [6].

Dengan fokus pada Facebook dan SIAKAD UNIRAYA, penelitian ini juga bertujuan untuk memberikan pemahaman yang lebih mendalam mengenai kerentanan spesifik yang mungkin terdapat pada kedua platform tersebut, serta memberikan rekomendasi yang disesuaikan untuk meningkatkan keamanan di lingkungan tersebut. Hal ini diharapkan dapat memberikan kontribusi yang signifikan dalam upaya pencegahan phishing di lingkungan pendidikan dan media sosial [7]. Penelitian ini juga dikerjakan dalam ruang lingkup edukatif dan terbatas, tanpa melibatkan data asli maupun penyebaran tautan secara publik, sehingga tetap menjaga aspek etika dan legalitas dalam prosesnya. Dengan demikian, simulasi ini diharapkan dapat menjadi langkah awal dalam membangun literasi digital dan kesadaran keamanan siber di tengah masyarakat.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini menggunakan metode eksperimen, yaitu suatu metode penelitian yang dilakukan dengan sengaja memanipulasi satu atau lebih variabel dalam kondisi yang terkendali untuk mengetahui pengaruhnya terhadap variabel lain [8]. Pemilihan metode eksperimen dilakukan karena dianggap paling relevan dalam mengamati langsung proses simulasi serangan phishing secara teknis dan sistematis. Penelitian ini difokuskan pada penerapan dua alat utama, yaitu Zphisher dan Ngrok, dalam membuat dan menguji situs tiruan (phishing) yang menyerupai tampilan asli situs Facebook dan SIAKAD UNIRAYA.

Secara umum, tahapan dalam penelitian ini dimulai dengan proses persiapan lingkungan eksperimen. Peneliti menyiapkan perangkat lunak yang dibutuhkan, seperti sistem operasi Kali Linux, terminal, Zphisher, dan layanan Ngrok. Setelah itu, tahap simulasi dimulai dengan dua skenario berbeda, masing-masing menggunakan alat yang berbeda namun memiliki tujuan sama, yaitu menciptakan situs phishing dan mengamati respons sistem terhadap data login fiktif yang dimasukkan.

Tahap berikutnya adalah pengamatan dan pencatatan data. Peneliti mengamati bagaimana masing-masing alat menghasilkan halaman tiruan, seberapa mirip tampilannya dengan situs aslinya, serta kecepatan dan akurasi alat dalam menangkap data login. Pengamatan ini dilakukan melalui terminal dan antarmuka masing-masing alat secara real time. Seluruh simulasi dilakukan dalam kondisi lingkungan terbatas, artinya tidak ada penyebaran tautan ke pihak luar dan tidak ada keterlibatan pengguna asli. Peneliti hanya menggunakan data login fiktif untuk keperluan pengujian. Oleh karena itu, hasil dari simulasi ini merupakan hasil dari proses teknis yang dikendalikan sepenuhnya oleh peneliti, dan tidak dipengaruhi oleh faktor eksternal seperti perilaku pengguna atau kondisi jaringan publik.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

Untuk memperjelas proses penelitian yang dilakukan, berikut ini disajikan diagram alur yang menggambarkan tahapan eksperimen secara sistematis:

Gambar 1. Gambaran Tahapan Penelitian

Untuk memberikan pemahaman yang lebih jelas mengenai proses yang dilakukan dalam penelitian ini, berikut disajikan penjabaran singkat dari masing-masing tahapan yang telah digambarkan dalam diagram alur. Setiap tahap memiliki peran penting dalam mendukung kelancaran dan validitas proses eksperimen phishing yang dilakukan. Adapun penjelasannya adalah sebagai berikut:

1. **Persiapan Lingkungan**: Peneliti menyiapkan tools utama (Zphisher dan Ngrok) dalam sistem operasi Kali Linux. Tahapan ini penting untuk memastikan semua kebutuhan teknis tersedia.

2. **Simulasi Skenario:** Simulasi dilakukan dalam dua skenario: pertama menggunakan **Zphisher** untuk membuat situs tiruan otomatis, dan kedua menggunakan **Ngrok** untuk membuat akses publik ke situs lokal. Keduanya bertujuan menciptakan lingkungan serangan phishing.

3. **Pengamatan & Pencatatan Data:** Peneliti Peneliti mengamati hasil dari kedua alat yang digunakan dalam simulasi dengan memperhatikan beberapa aspek penting, seperti kualitas tampilan situs tiruan yang dihasilkan, kecepatan alat dalam menangkap data login fiktif yang dimasukkan, serta tingkat akurasi masing-masing alat dalam menduplikasi tampilan situs asli dan mencatat input pengguna secara tepat.

4. **Simulasi dalam Lingkup Tertutup:** Simulasi tidak menyebar ke dunia luar. Hanya digunakan data palsu, tanpa intervensi dari pengguna asli, sehingga eksperimen sepenuhnya terkendali.

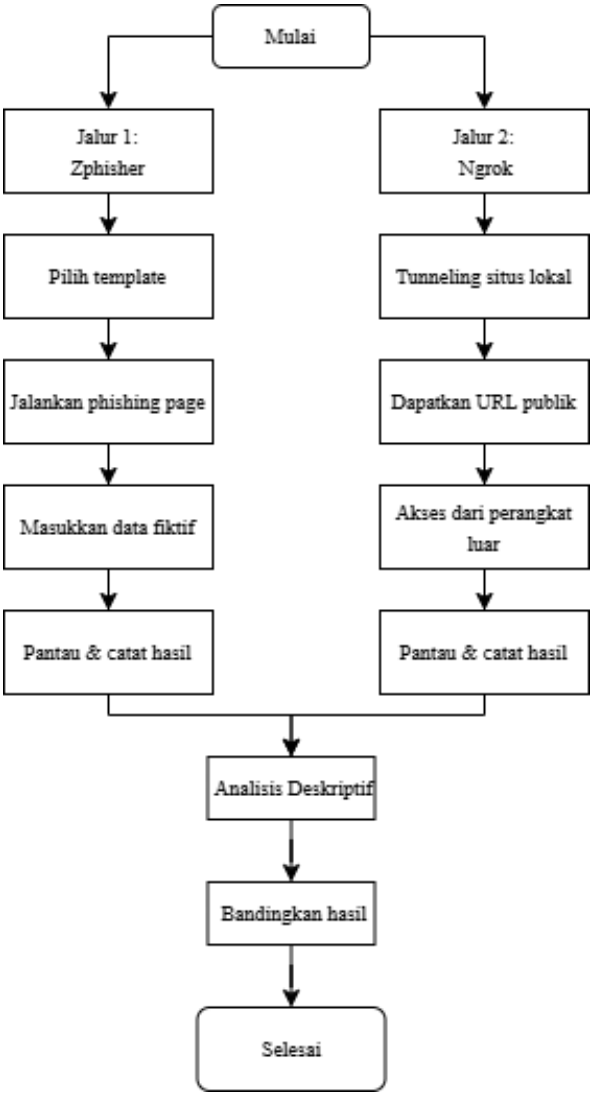
2.2 Penerapan dan Pengujian Metode

Penerapan metode eksperimen dalam penelitian ini dilakukan dengan membagi simulasi ke dalam dua jalur. Jalur pertama menggunakan Zphisher sebagai alat utama. Zphisher memiliki kemampuan untuk membuat halaman login tiruan secara otomatis berdasarkan template situs populer, seperti Facebook atau sistem informasi akademik. Dalam penelitian ini, peneliti memilih template Facebook dan menyesuaikannya dengan kebutuhan simulasi. Zphisher dijalankan dalam terminal pada sistem operasi Kali Linux. Setelah halaman phishing berhasil dibuat, peneliti

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

memasukkan data login fiktif untuk melihat apakah informasi tersebut berhasil ditangkap oleh sistem. Selain itu, diamati pula sejauh mana tampilan halaman menyerupai situs asli dan seberapa cepat alat menerima data input.

Jalur kedua menggunakan Ngrok yang dikombinasikan dengan metode tunneling untuk membuka akses situs lokal ke jaringan publik. Ngrok memberikan URL publik sementara yang bisa digunakan untuk mengakses halaman phishing dari perangkat lain atau jaringan luar [9]. Peneliti memanfaatkan jalur ini untuk mengamati apakah situs phishing tetap stabil saat diakses dari luar serta apakah data login tetap berhasil dikirim dan dicatat oleh sistem. Gambaran dari pengujian kedua jalur dapat dilihat pada gambar berikut:



Gambar 2. Diagram alur pengujian

Dalam konteks ini, Ngrok juga menggambarkan bagaimana pelaku siber dapat menyamarkan alamat IP asli mereka melalui jalur tunneling dan menyembunyikan identitas lokasi server [10]. Setiap tahapan metode diuji dari segi efektivitas dan keamanan. Zphisher dinilai dari segi kecepatan pembuatan situs phishing dan kemudahan penggunaan, sedangkan Ngrok diuji dari segi aksesibilitas lintas jaringan dan kestabilan koneksi. Semua data yang dihasilkan berupa tangkapan username dan password uji coba dicatat untuk dianalisis secara deskriptif, tanpa proses kuantitatif. Analisis deskriptif digunakan untuk membandingkan kelebihan dan kekurangan masing-masing alat dari sudut pandang teknis dan keamanan [11].

Penelitian ini dilakukan dengan mengedepankan prinsip etika. Tidak ada data asli yang digunakan dan tidak ada tautan phishing yang disebarluaskan ke publik. Fokus penelitian adalah untuk meningkatkan pemahaman teknis mengenai metode phishing sebagai bentuk edukasi dalam konteks keamanan siber. Dengan metode ini, diharapkan para pengelola sistem dan pengguna awam dapat lebih waspada terhadap berbagai potensi serangan di dunia maya [12].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

3. HASIL DAN PEMBAHASAN

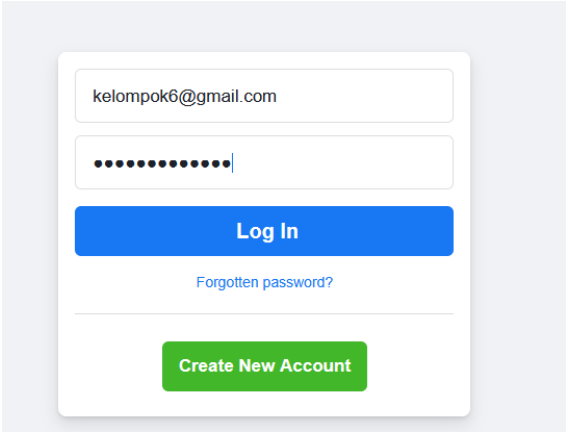
Pada bagian ini, akan dipaparkan hasil dari dua eksperimen simulasi phishing yang dilakukan menggunakan dua alat berbeda, yaitu Zphisher dan Ngrok. Setiap eksperimen dirancang secara terpisah, meskipun pendekatannya serupa, yaitu dengan membuat situs tiruan yang menyerupai situs resmi untuk melihat apakah data login uji coba bisa ditangkap. Tujuan dari simulasi ini adalah untuk mengamati sejauh mana kedua alat ini efektif dalam meniru tampilan situs asli dan menangkap informasi login, serta untuk memahami potensi risiko apabila teknologi ini disalahgunakan oleh pihak yang tidak bertanggung jawab [13].

3.1 Simulasi Phishing Menggunakan Zphisher

Eksperimen pertama dilakukan menggunakan Zphisher, yaitu sebuah alat open-source yang dirancang untuk memudahkan pembuatan halaman phishing berbasis template. Dalam eksperimen ini, peneliti menggunakan sistem operasi Kali Linux untuk menjalankan alat tersebut. Langkah awal dimulai dengan membuka terminal dan masuk ke direktori Zphisher menggunakan perintah *cd zphisher/*, kemudian menjalankan skrip *./zphisher.sh* untuk memulai program. Setelah Zphisher berjalan, muncul daftar situs yang bisa ditiru tampilannya. Peneliti memilih Facebook sebagai target simulasi karena merupakan salah satu situs yang paling umum dijadikan sasaran dalam praktik phishing [14].

Gambar 3. Munculnya Link Cloudflared

Setelah memilih Facebook, Zphisher menampilkan beberapa opsi tampilan halaman login yang berbeda. Peneliti memilih tampilan klasik atau tradisional karena lebih sederhana namun tetap menyerupai versi aslinya. Selanjutnya, Zphisher memberikan pilihan untuk layanan tunneling atau port forwarding agar situs phishing bisa diakses dari jaringan luar. Dalam eksperimen ini, peneliti menggunakan layanan Cloudflared, yang secara otomatis menghasilkan beberapa URL publik. URL ini dapat dibuka di perangkat lain untuk mengakses halaman phishing.

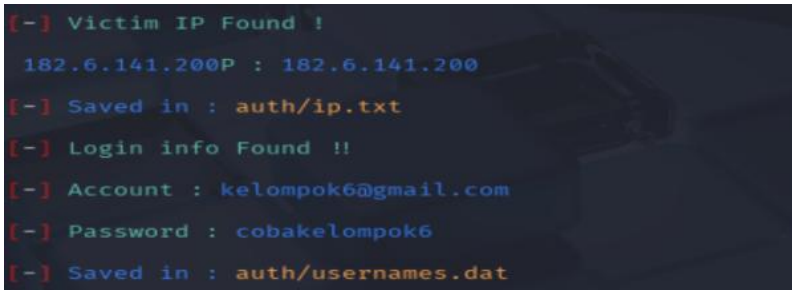


Gambar 4. Tampilan Halaman Login Palsu Facebook

Setelah layanan tunneling aktif, di terminal muncul status ***"Waiting for Login Info"*** yang menandakan bahwa sistem sedang menunggu data dari pengguna yang membuka halaman phishing. Peneliti kemudian mengakses salah satu link yang telah dibuat dan membuka halaman login palsu Facebook melalui browser. Halaman tersebut menampilkan kolom email dan kata sandi, tombol login, serta elemen lain seperti tautan untuk lupa kata sandi dan pembuatan akun baru.

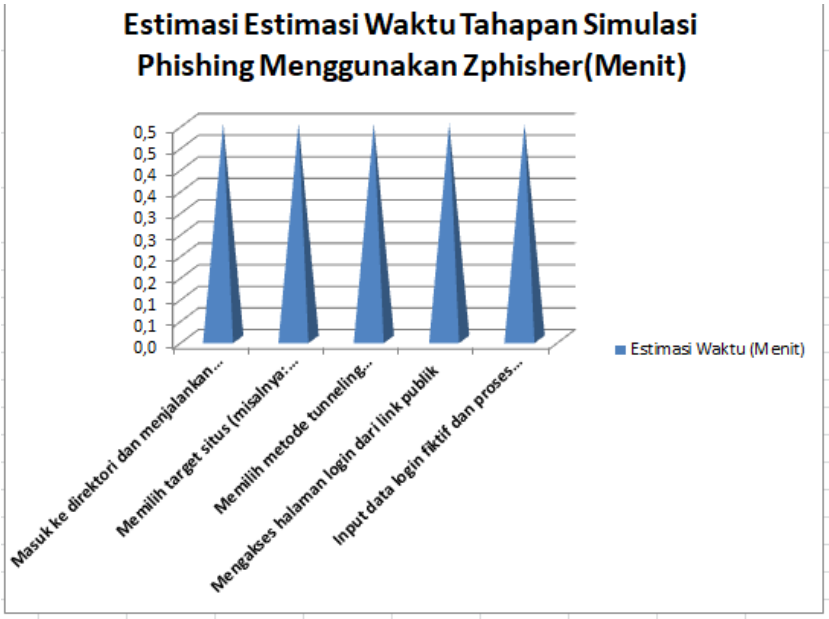
Peneliti menguji fungsionalitas halaman ini dengan memasukkan data uji coba berupa email *kelompok6@gmail.com* dan kata sandi ***cobakelompok6***. Setelah tombol login ditekan, data yang dimasukkan langsung muncul di terminal Zphisher, lengkap dengan alamat IP pengguna yang mengakses halaman tersebut, yaitu ***182.6.141.200***.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390



Gambar 5. Data Login Tertangkap oleh Zphisher

Informasi ini juga secara otomatis tersimpan dalam file ip.txt untuk alamat IP dan usernames.dat untuk data login. Proses ini dilakukan sepenuhnya di lingkungan lokal tanpa membagikan link kepada pihak luar, dan semua data yang dimasukkan bersifat fiktif serta hanya untuk keperluan pengujian internal.



Gambar 6. Grafik Estimasi Waktu Tahapan Simulasi Phishing Menggunakan Zphisher

3.2 Simulasi Phishing menggunakan Ngrok

Berisi hasil implementasi penerapan metode, ataupun hasil dari pengujian metode. Simulasi dimulai dengan proses instalasi dan konfigurasi awal Ngrok di sistem operasi Linux. Peneliti mengekstrak file instalasi menggunakan perintah *sudo tar -xvzf ngrok-stable-linux-amd64.tgz* lalu menyalin hasil ekstraksinya ke direktori */usr/local/bin/* agar Ngrok dapat dijalankan dari terminal. Setelah instalasi selesai, perintah *ngrok config add-authtoken [token]* digunakan untuk menambahkan authtoken ke dalam konfigurasi sistem. Authtoken ini berfungsi sebagai autentikasi pengguna agar dapat menggunakan fitur-fitur penuh dari Ngrok, termasuk pembuatan tunneling publik secara aman dan efisien.

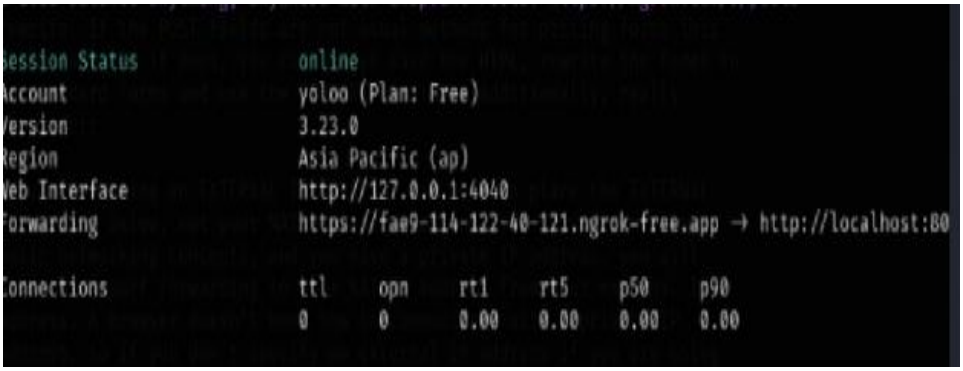
Ketika peneliti mencoba menjalankan aplikasi terminal dengan hak akses root, muncul jendela otentikasi sistem yang meminta password administrator. Ini merupakan langkah standar dalam sistem operasi Linux untuk mencegah eksekusi tindakan administratif tanpa otorisasi yang sah. Setelah berhasil masuk sebagai root, peneliti menjalankan perintah *setoolkit* untuk membuka *Social-Engineer Toolkit (SET)*. SET adalah alat yang banyak digunakan dalam simulasi serangan rekayasa sosial seperti phishing, spear-phishing, dan lainnya karena kemampuannya dalam membuat dan menjalankan situs tiruan secara efisien [15].

Langkah selanjutnya adalah membuka situs resmi yang menjadi target tiruan, dalam hal ini halaman login Sistem Informasi Akademik (SIAKAD) milik UNIRAYA, yang diakses melalui URL ***siakad.uniraya.ac.id***. URL ini kemudian disalin dan digunakan sebagai referensi visual dan struktural dalam pembuatan halaman phishing. Proses ini penting agar hasil tampilan akhir menyerupai situs aslinya sehingga pengguna awam tidak akan langsung menyadari perbedaannya [16].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

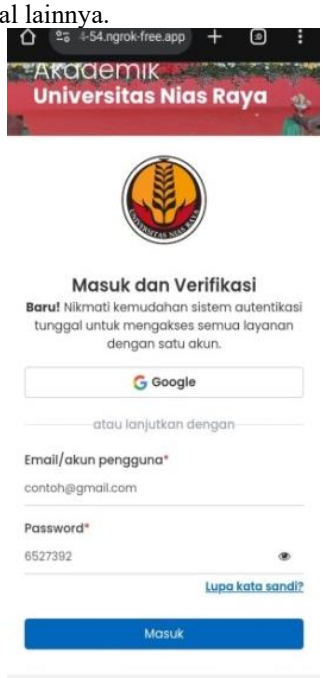
Gambar 7. Menjalankan Ngrok

Setelah proses replikasi halaman dilakukan secara otomatis melalui opsi dalam SET, sehingga tidak ada pembuatan manual HTML yang dilakukan dan tidak memerlukan konfigurasi rumit, peneliti kemudian keluar dari mode root dan membuka terminal biasa untuk menjalankan server lokal. Namun, dalam praktiknya, server lokal PHP tidak diaktifkan secara terpisah karena halaman phishing langsung dijalankan menggunakan layanan Ngrok. *Perintah ngrok http 80* digunakan untuk membuat tunnel dari sistem lokal ke jaringan publik, dan Ngrok menyediakan satu atau beberapa URL publik sementara, seperti https://fae9-114-112-40-121.ngrok-free.app, yang dapat diakses dari mana saja.



Gambar 8. Munculnya Link Forwarding

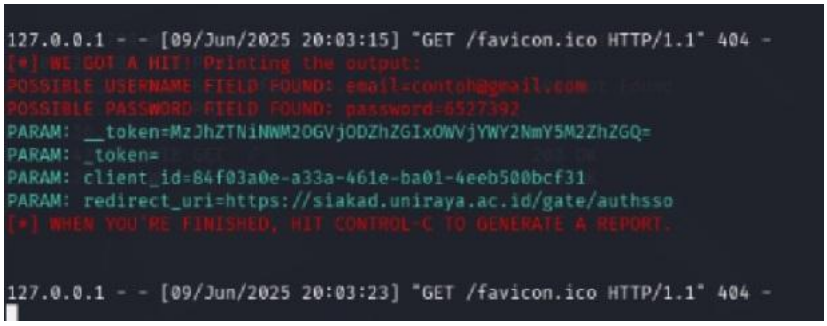
Setelah link publik tersedia, peneliti membuka URL tersebut melalui browser untuk memastikan bahwa situs phishing dapat dimuat dengan baik. Halaman login yang ditampilkan sangat menyerupai tampilan asli, termasuk letak kolom username, password, dan elemen visual lainnya.



Gambar 9. Halaman Login Tiruan

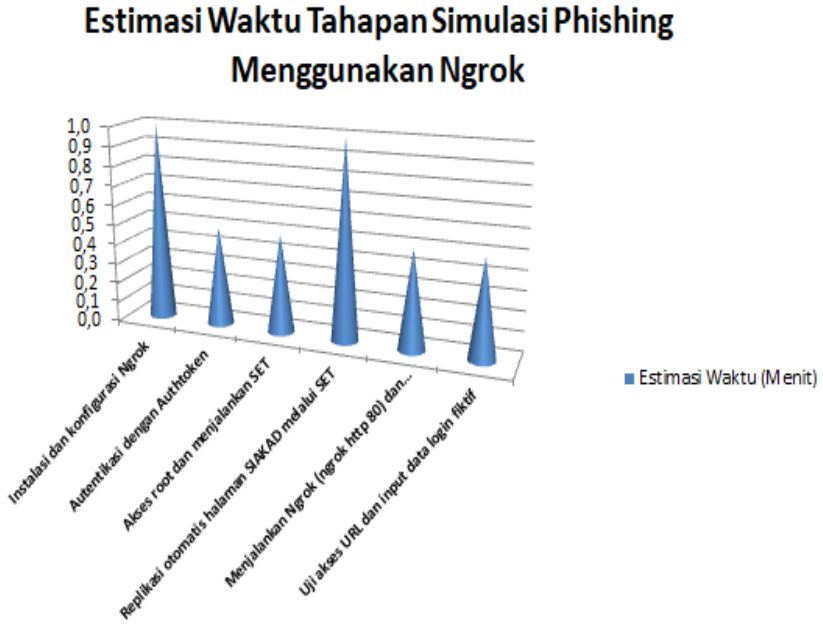
Pengujian dilakukan dengan mengisi form login menggunakan data fiktif seperti email **contoh@gmail.com** dan kata sandi **6527392**. Ketika tombol login ditekan, data tersebut langsung ditampilkan di terminal secara real-time, termasuk informasi alamat IP perangkat pengakses.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390



Gambar 10. Data Tertangkap di Terminal

Terakhir, sistem mencatat data login yang masuk ke dalam file seperti *usernames.txt* untuk menyimpan kombinasi email dan password, serta *ip.txt* untuk merekam alamat IP pengakses. Proses ini menandakan bahwa seluruh tahapan simulasi berjalan dengan lancar dan situs phishing berhasil diakses secara publik dengan dukungan layanan tunneling dari Ngrok. Proses ini berlangsung dalam waktu singkat dan berjalan stabil pada perangkat dengan spesifikasi standar, menunjukkan bahwa metode ini efektif digunakan untuk menangkap informasi login tanpa perlu menyewa server eksternal maupun melakukan konfigurasi lanjutan [17].



Gambar 11. Grafik Estimasi Waktu Tahapan Simulasi Phishing Menggunakan Ngrok

3.3 Perbandingan Antara Zphisher dan Ngrok

Berisi hasil implementasi penerapan metode, ataupun hasil dari pengujian metode. Zphisher dan Ngrok merupakan dua pendekatan yang digunakan dalam simulasi serangan phishing, namun keduanya memiliki perbedaan mendasar dari segi kemudahan penggunaan, fleksibilitas, dan tingkat kontrol terhadap halaman phishing yang dibuat. Zphisher hadir sebagai alat serba guna berbasis antarmuka terminal yang menyediakan berbagai template halaman login dari situs populer seperti Facebook, Instagram, Twitter, dan lainnya. Dalam praktiknya, Zphisher sangat cocok untuk pengguna yang menginginkan solusi cepat karena proses pembuatan halaman phishing hanya memerlukan beberapa langkah sederhana melalui pilihan otomatis. Dengan tampilan antarmuka berbasis menu, pengguna cukup memilih target situs dan jenis halaman login, lalu Zphisher secara otomatis akan menghasilkan URL publik melalui layanan tunneling seperti Cloudflared [18].

Sementara itu, metode yang menggunakan Ngrok menawarkan pendekatan yang lebih fleksibel namun tetap otomatis. Dalam eksperimen ini, Ngrok digunakan untuk meng-online-kan situs phishing yang dibuat melalui pilihan otomatis dalam Social-Engineer Toolkit (SET). Tidak ada pengeditan HTML secara manual maupun pengaktifan server lokal yang diperlukan. Kelebihan dari metode ini adalah pengguna tetap dapat memperoleh URL publik dan tampilan tiruan situs yang sesuai dengan pilihan target yang tersedia. Prosesnya tetap memerlukan pemahaman dasar tentang terminal, namun tidak menuntut kemampuan pemrograman lanjutan.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

Tabel 1. Alur Proses Simulasi Phishing

Proses Simulasi Zphisher		Proses Simulasi Zphisher	
1.	Buka terminal & masuk ke direktori Zphisher	1.	Install & konfigurasikan Ngrok
2.	Jalankan skrip: *./zphisher.sh*	2.	Tambah authtoken Ngrok
3.	Pilih target situs (misalnya Facebook)	3.	Jalankan SET *(Social Engineering Toolkit)*
4.	Pilih tampilan halaman login	4.	Pilih opsi pembuatan situs phishing
5.	Pilih metode tunneling (Cloudflared)	5.	Pilih target & tampilan (otomatis, tanpa HTML manual)
6.	Zphisher membuat link phishing	6.	Jalankan perintah: *ngrok http 80*
7.	Akses link & masukkan data uji coba	7.	Akses link publik yang muncul
8.	Data login muncul di terminal & tersimpan otomatis	8.	Data login tampil di terminal & tersimpan otomatis

Dari sisi kemudahan dan kecepatan, Zphisher jelas lebih unggul karena pengguna hanya perlu memilih beberapa opsi tanpa harus menulis kode atau mengatur konfigurasi server secara manual. Proses otomatisasi ini membuat Zphisher sangat ideal digunakan untuk simulasi dasar atau pembelajaran awal mengenai teknik phishing. Namun, kekurangannya terletak pada keterbatasan variasi tampilan dan kurangnya kontrol terhadap halaman phishing yang dihasilkan. Berbeda dengan itu, penggunaan Ngrok memberikan keleluasaan bagi peneliti untuk mendesain halaman secara detail dan menjalankannya menggunakan metode tunneling yang lebih aman dan stabil, meskipun memerlukan waktu dan keterampilan teknis yang lebih tinggi.

Dalam hal hasil akhir, kedua metode sama-sama mampu menangkap data login fiktif yang dimasukkan oleh pengguna, termasuk username, password, dan alamat IP. Namun, pada simulasi Zphisher, proses ini berlangsung secara instan dan seluruh data langsung muncul di terminal setelah korban menekan tombol login. Sedangkan dalam simulasi dengan Ngrok, prosesnya melalui beberapa tahap tambahan seperti konfigurasi SET dan pembuatan manual halaman tiruan, namun memberikan hasil yang sama akuratnya. Hal ini menunjukkan bahwa efektivitas keduanya dalam menangkap data tidak terlalu berbeda, yang membedakan hanyalah pendekatan, tingkat kompleksitas, dan pengalaman pengguna selama proses pembuatan.

Secara umum, Zphisher lebih sesuai untuk kebutuhan simulasi cepat dan praktis, sedangkan Ngrok memberikan kebebasan lebih besar untuk pengembangan yang lebih kompleks dan mendalam. Pilihan antara keduanya sangat bergantung pada tujuan simulasi, tingkat keahlian pengguna, dan jenis target yang ingin ditiru. Baik Zphisher maupun Ngrok, jika digunakan tanpa pengawasan dan tidak sesuai etika, memiliki potensi untuk disalahgunakan, sehingga dalam konteks penelitian seperti ini, penggunaan alat-alat tersebut harus tetap berada dalam koridor akademik dan etika profesional.

Dari sisi efisiensi, kedua metode memiliki waktu penyelesaian yang hampir sama, yaitu sekitar 3 hingga 5 menit sejak program dijalankan hingga situs phishing aktif dan dapat diakses secara publik. Dalam masing-masing metode, peneliti melakukan tiga kali login uji coba dan seluruh data berhasil ditangkap tanpa kendala teknis. Sistem tidak menunjukkan peningkatan beban atau gangguan selama proses berlangsung, menunjukkan bahwa simulasi ini dapat dijalankan dengan lancar bahkan pada perangkat dengan spesifikasi menengah.

3.4 Implikasi Temuan dan Rekomendasi Keamanan

Temuan dari simulasi phishing menggunakan Zphisher dan Ngrok menunjukkan bahwa kedua alat ini memiliki kemampuan tinggi dalam meniru tampilan situs asli dan menangkap data login fiktif dengan efektif. Hal ini memberikan gambaran bahwa serangan phishing dapat dilakukan oleh siapa saja yang memiliki akses ke alat tersebut, tanpa harus memiliki kemampuan teknis tingkat lanjut. Dalam praktiknya, Zphisher bahkan hanya membutuhkan beberapa langkah untuk menghasilkan link phishing dengan tampilan yang meyakinkan. Situasi ini menjadi perhatian serius karena menunjukkan betapa mudahnya serangan semacam ini dilakukan apabila jatuh ke tangan yang salah [19].

Kemampuan Zphisher dalam menyediakan template situs populer secara otomatis, dan kemudahan Ngrok dalam membuka akses situs lokal ke jaringan publik, menandakan bahwa risiko phishing tidak hanya datang dari aktor profesional, tetapi juga dari pengguna biasa yang memiliki niat buruk. Keduanya memberikan potensi penyalahgunaan yang besar, terutama jika digunakan tanpa pengawasan atau tanpa pemahaman mengenai etika dan hukum dunia digital [20]. Oleh karena itu, temuan ini menjadi pengingat penting bagi institusi pendidikan, organisasi, dan pengguna internet pada umumnya bahwa kewaspadaan terhadap ancaman phishing perlu ditingkatkan.

Salah satu implikasi penting dari temuan ini adalah perlunya peningkatan literasi keamanan digital di semua kalangan, khususnya pada sektor pendidikan dan sosial media yang menjadi target utama dalam simulasi ini. Edukasi yang tepat mengenai cara mengenali situs palsu, pentingnya memeriksa URL, serta mendorong penggunaan fitur keamanan tambahan seperti autentikasi dua faktor (2FA), merupakan langkah awal yang dapat mengurangi risiko menjadi korban phishing [21].

Sebagai rekomendasi, institusi penyedia layanan digital, baik milik pemerintah, pendidikan, maupun swasta, disarankan untuk melakukan simulasi keamanan secara berkala guna menguji ketahanan sistem mereka terhadap potensi serangan sosial engineering. Selain itu, setiap situs resmi perlu dilengkapi dengan sertifikat SSL/TLS yang sah serta

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

fitur deteksi aktivitas mencurigakan secara otomatis. Penggunaan firewall aplikasi web *(Web Application Firewall/WAF)* dan sistem monitoring log juga dapat membantu dalam mengidentifikasi akses yang tidak biasa atau berpotensi berbahaya [22].

Untuk pengguna internet secara individu, penting untuk mengembangkan kebiasaan digital yang aman, seperti tidak mengklik tautan dari sumber yang tidak dikenal, menghindari login melalui link yang mencurigakan, dan menggunakan pengelola kata sandi agar setiap akun memiliki kredensial yang unik dan kuat. Selain itu, pemerintah juga didorong untuk memperketat regulasi terhadap peredaran alat-alat berisiko tinggi yang dapat disalahgunakan, serta menyediakan platform pengaduan yang mudah diakses oleh masyarakat ketika mereka menemukan potensi phishing atau penipuan digital lainnya [23].

Simulasi yang dilakukan dalam penelitian ini murni bertujuan untuk edukasi dan penguatan literasi keamanan digital, bukan untuk eksploitasi atau tindakan ilegal. Seluruh proses dilakukan di lingkungan terbatas tanpa melibatkan pihak luar, dan semua data yang digunakan bersifat fiktif. Peneliti tidak menyebarluaskan link phishing ke publik serta tidak menyimpan data pribadi siapa pun. Penelitian ini mengikuti prinsip *ethical hacking* dan disusun dalam konteks akademik untuk meningkatkan kesadaran tentang potensi ancaman serangan phishing dan pentingnya perlindungan data pribadi [24].

Secara keseluruhan, hasil dari simulasi ini menekankan bahwa upaya pencegahan terhadap serangan phishing tidak cukup hanya pada aspek teknis, tetapi juga membutuhkan pendekatan edukatif dan kebijakan yang kuat. Kolaborasi antara pengguna, penyedia layanan digital, serta lembaga pengawas keamanan siber menjadi kunci untuk menciptakan ruang digital yang lebih aman dan sadar risiko.

4. KESIMPULAN

Berdasarkan hasil simulasi yang dilakukan menggunakan Zphisher dan Ngrok, dapat disimpulkan bahwa kedua alat ini sama-sama efektif dalam membuat situs phishing dan menangkap data login fiktif. Zphisher terbukti lebih mudah digunakan karena sudah menyediakan berbagai template halaman login secara otomatis, sehingga pengguna tidak perlu memiliki keterampilan teknis yang tinggi. Sementara itu, Ngrok menawarkan fleksibilitas yang lebih besar karena memberikan kontrol lebih detail dalam proses pembuatan situs tiruan dan akses jaringan publik yang stabil. Meskipun pendekatannya berbeda, keduanya berhasil menunjukkan bagaimana phishing dapat dilakukan dengan cepat dan akurat. Hasil ini memperlihatkan bahwa serangan phishing bukan hanya dapat dilakukan oleh pelaku profesional, tetapi juga oleh siapa saja yang memiliki akses ke alat yang tersedia secara bebas. Hal ini menunjukkan bahwa risiko serangan phishing sangat tinggi apabila tidak disertai dengan edukasi dan langkah mitigasi yang tepat. Temuan dari simulasi ini memperkuat pentingnya peningkatan kewaspadaan dan literasi keamanan digital, terutama di lingkungan pendidikan dan media sosial yang rentan menjadi target. Penelitian ini dilakukan sepenuhnya untuk tujuan edukasi dan tidak melibatkan data pribadi siapa pun. Semua data yang digunakan bersifat fiktif dan tidak disebarluaskan. Oleh karena itu, penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik mengenai cara kerja serangan phishing serta mendorong kesadaran akan pentingnya menjaga keamanan data pribadi di era digital. Selain itu, diharapkan juga dapat menjadi referensi awal bagi pengembangan sistem pertahanan siber yang lebih baik di lingkungan akademik..

REFERENCES

[1] M. N. Trisolvena and N. H. Saputra, “Phishing Cyber Security Threats,” *J. Improsci*, vol. 2, no. 1, pp. 38–48, 2024, doi: 10.62885/improsci.v2i1.440.

[2] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, “Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial,” *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/pjise.v1i4.2753.

[3] T. Ginanjar Laksana and S. Mulyani, “Faktor-Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan,” *J. Huk. Prioris*, vol. 11, no. 2, pp. 136–160, 2024, doi: 10.25105/prio.v11i2.18960.

[4] D. A. Rismasari, “DALAM MENCEGAH KEBOCORAN DATA NASABAH PERBANKAN DIGITAL MELALUI PESAN PHISHING DI PENDAHULUAN Di era digitalisasi , teknologi dan informasi berkembang sangat pesat dan cepat sehingga membawa dampak pada kehidupan masyarakat sehari-hari (Siahaan , 2022).,” *Jubaedah J. Pengabdi. dan Edukasi Sekol.*, vol. 5, pp. 41–50, 2025.

[5] R. Hidayat and N. Anwar, “Forensic Analysis of Web Phishing and Social Engineering Using the National Institute of Standards and Technology Method Case Study of Facebook Account Data Theft,” *J. Digit. Secur. Forensics*, vol. 1, pp. 12–25, 2024, doi: 10.29121/DigiSecForensics.v1.i1.202.

[6] 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.

[7] R. Lesmana and M. I. P. Nasution, “Kebocoran Data di Media Sosial : Analisis Pola dan Strategi Pencegahannya,” *Socius J. Adm. Publik*, vol. 2, no. May, pp. 123–128, 2025.

[8] S. N. Zyra, T. P. Alamsyah, and R. Yuliana, “Penggunaan E-Learning Berbasis Edmodo Terhadap Hasil Belajar Kelas 4 Sekolah Dasar,” *J. PGSD J. Ilm. Pendidik. Guru Sekol. Dasar*, vol. 15, no. 2, pp. 97–106, 2022, doi: 10.33369/pgsd.15.2.97-106.

[9] A. Widyanto, Y. Aprizal, A. Wardani, and A. Kegiatan, “Prosiding Seminar Nasional CORISINDO 2021 Pengabdian Kepada Masyarakat Pengenalan dan Pengaplikasian Tunelling (ngrok.com) Bagi Siswa SMA Guna Mengakses Aplikasi Berbasis Web,” *Semin. Nas. CORISINDO 2021*, pp. 240–245, 2021, [Online]. Available: https://www.ngrok.com.

[10] R. Parlika, H. Khariono, H. Ananta Kusuma, M. Risalul Abrori, and M. Ainur Rofik, “Implementasi Akses Mysql dan Web Server Lokal

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 236-246
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.390

Melalui Jaringan Internet Menggunakan Ngrok," *JIKO (Jurnal Inform. dan Komputer)*, vol. 3, no. 3, pp. 131–136, 2020, doi: 10.33387/jiko.v3i3.1799.
[11] Sutarti, Siswanto, and A. Bachtiar, "Analisis Web Phishing Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router Mikrotik," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 10, no. 1, pp. 71–83, 2023, doi: 10.30656/prosisko.v10i1.7048.
[12] F. G. Lubis, "Latar Belakang Kemajuan teknologi digital telah mengubah pola interaksi sosial, bisnis, dan pemerintahan di seluruh dunia. Dunia maya, atau," *J. Huk. dan Kewarganegaraan*, vol. 6, no. 7, 2024.
[13] J. S. Tharani and N. A. G. Arachchilage, "Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach," *Secur. Priv.*, vol. 3, no. 5, pp. 1–15, 2020, doi: 10.1002/spy2.120.
[14] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *Automata*, vol. 2, no. 2, pp. 1–4, 2021.
[15] 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.
[16] S. Wahyuni, I. Murti, and I. Dwitawati, "Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 1, pp. 49–55, 2022.
[17] S. R. Wicaksono, *TUNNELING dan P2P Teori dan Studi Kasus*, no. August 2021. 2023. doi: 10.5281/zenodo.7659697.
[18] G. A. Kothamasu, S. K. A. Venkata, Y. Pemmasani, and S. Mathi, "An Investigation on Vulnerability Analysis of Phishing Attacks and Countermeasures," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 2, pp. 333–340, 2023, doi: 10.18280/ijsse.130215.
[19] N. Afrianto *et al.*, "Perancangan Jaringan Vpn Dan Keamanan Data Menggunakan Tunelling Pada Laboratorium Komputer UIN Sunan Kalijaga Yogyakarta," *JUTIS (Jurnal Tek. Inform. Unis)*, vol. 12, no. 1, pp. 27–38, 2024.
[20] Y. Fitriani and R. Pakpahan, "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace," *Cakrawala-Jurnal Hum.*, vol. 20, no. 1, pp. 21–27, 2020, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala
[21] P. Phising and D. A. N. Cara, "Pengenalan phising dan cara penanganannya," *APPA J. Pengabdi. Kpd. Masy.*, vol. 2, no. 5, pp. 587–589, 2025.
[22] M. F. Rizqi, R. Tulloh, and N. Djibran, "Implementasi Web Application Firewall untuk Melindungi Aplikasi Web dari Serangan Malware," *J. Inform. Univ. Pamulang*, vol. 8, no. 2, pp. 341–348, 2023, doi: 10.32493/informatika.v8i2.33691.
[23] W. B. M. Setiyawan, E. Churniawan, and F. S. Faried, "Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State Sovereignty of the Republic of Indonesia," *urnal USM Law*, vol. 3, no. 2, pp. 275–295, 2020.
[24] D. Chirzah and E. Y. Al-fadli, "Studi Perbandingan,Pengetahuan,Dan Perilaku Cyber Security Di Indonesia," *J. Trends. Vol. 01 Nomor 01 Tahun 2023*, vol. 01, pp. 19–24, 2023, [Online]. Available: https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/290/271