Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

Analisis Keamanan Jaringan Sosial Media

Rakhmadi Rahman, Figra Dwi Kuncahya

Prodi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Juni 2024
Revisi Juni 2024
Diterima Juli 2024

Kata Kunci:
Keamanan Jaringan Media Sosial, Perlindungan Data Pribadi, Risiko Keamanan, Penggelabuan

*Penulis Korespondensi:
figradwi28@gmail.com

ABSTRAK

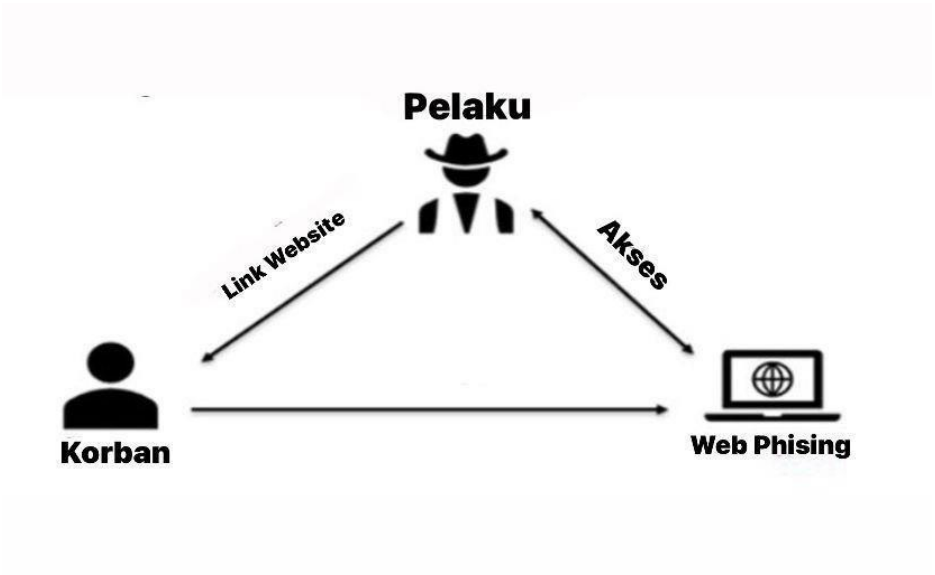
Pada era digital, penggunaan media sosial meningkat secara signifikan, namun hal ini juga meningkatkan risiko keamanan dan privasi. Penelitian ini menyajikan analisis keamanan jaringan media sosial yang berfokus pada perlindungan informasi pribadi pengguna. Penelitian menunjukkan bahwa sebagian besar pengguna tidak memahami kebijakan privasi media sosial dan bagaimana informasi pribadi mereka dilindungi. Oleh karena itu, penelitian ini dilakukan untuk menganalisis keamanan profil pengguna media sosial dari ancaman aktivitas pengumpulan informasi menggunakan metode intelijen sumber terbuka untuk membuat profil target. Hasil penelitian ini dapat membantu meningkatkan kesadaran pemilik data dan penyelenggara sistem elektronik untuk lebih memperhatikan keamanan sistem informasi terhadap data pribadi seseorang.

ABSTRACT

In the digital era, the use of social media has increased significantly, but this also increases security and privacy risks. This study presents a security analysis of social media networks that focuses on protecting users' personal information. Research shows that most users do not understand social media privacy policies. And how their personal information is protected. Therefore, this study analyzed the security of social media user profiles from the threat of information collection activities using open-source intelligence methods to profile targets. The results of this study can help increase awareness of data owners and electronic system organizers to pay more attention to the security of information systems for someone's data.

PENDAHULUAN

Aplikasi perangkat lunak telah menjadi bagian penting dari kehidupan sehari-hari para pengguna seiring dengan pesatnya kemajuan era digital. Ratusan ribu aplikasi dapat diunduh ke perangkat mobileberbasis Android di Google Play Store. Netflix, platform penyedia konten streaming terkemuka, adalah salah satu aplikasi yang menerima banyak ulasan pengguna. Media sosial adalah bagian penting dari kehidupan sehari-hari masyarakat. Secara umum, informasi media sosial digunakan sebagai sarana komunikasi, informasi, dan hiburan. Contoh media sosial yang paling umum adalah Instagram, TikTok, Facebook, Twitter, dan YouTube. Website atau situs adalah kumpulan halaman web beserta file pendukungnya yang disimpan di server web yang umumnya dapat diakses melalui Internet. Tautan palsu yang akan mengarahkan pengguna menuju halaman berbahaya dan berpotensi melakukan pencurian data pribadi.



Gambar 1. Skenario Phising

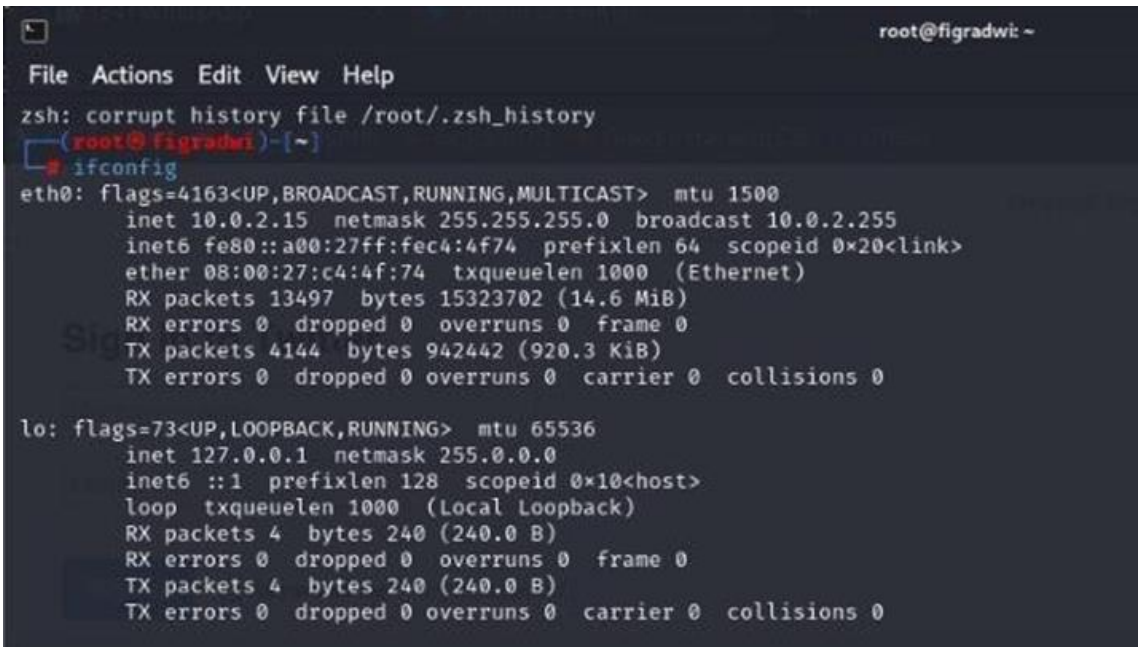
Pengimplementasian yang dilakukan ialah memeriksa keamanan informasi media sosial dengan menggunakan setoolkit, sebuah alat untuk phising. Hasil penelitian menunjukkan bahwa pengkloningan URL TWITTER akan menghasilkan halaman login TWITTER yang diakses dengan IP address pelaku phising. Ini menunjukkan bahwa pengujian mengkloning halaman TWITTER dengan metode phising berhasil. Hasil penelitian menunjukkan bahwa phising dapat terjadi di semua media sosial. Tujuan penelitian ini adalah untuk menguji situs media sosial dan melihat apakah situs tersebut dapat direplikasi sehingga terjadi pencurian data saat login. Oleh karena itu, pengujian dilakukan menggunakan setoolkit di Kali Linux.

METODE PENELITIAN

Pada penelitian ini menggunakan metode penelitian kuantitatif dan kualitatif. Pada penelitian kualitatif menggunakan studi pustaka untuk memahami mengenai metode phising yaitu mengancam keamanan informasi media sosial yang bertujuan untuk mencuri data-data penting. Kemudian pada penelitian kuantitatif menggunakan percobaan pada sebuah virtual machine Kali Linux kemudian diimplementasikan untuk menganalisis keamanan pada website media sosial yang tertuju seperti Instagram, Facebook, Twitter dan lainlainnya. Pada virtual machine tersebut nantinya akan muncul data login dari korban yang sudah mencoba mengakses website phising tersebut.

Percobaan Serangan Phising Mengecek Ip Address

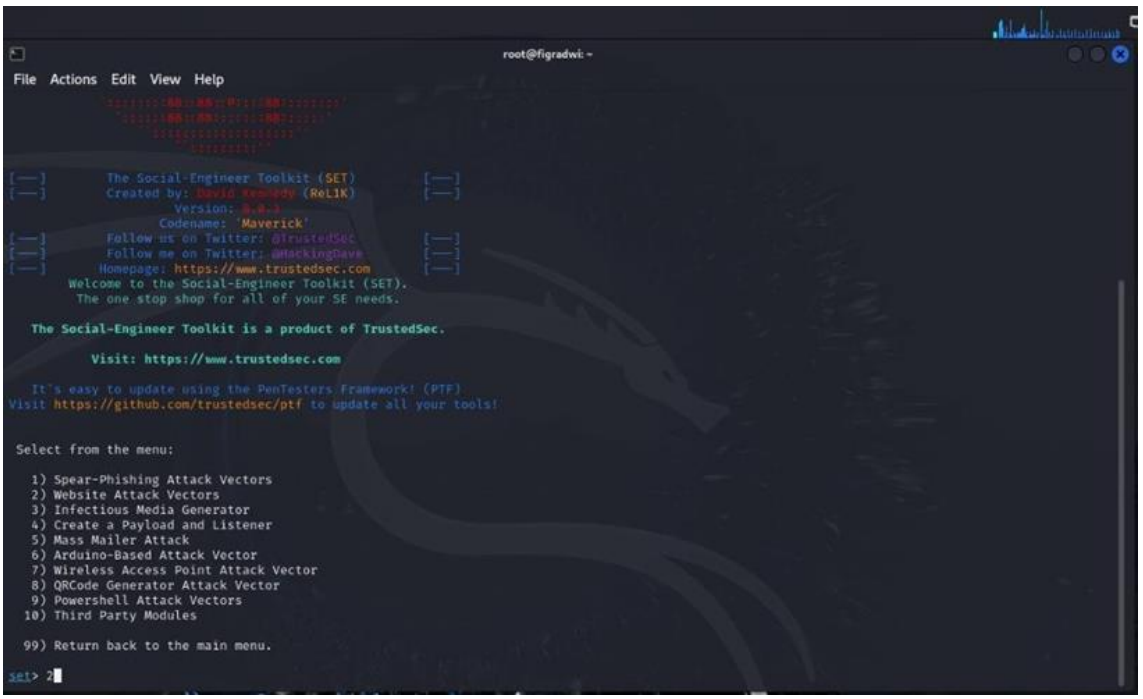
Setelah memasuki halaman Linux, langkah awal yang dilakukan adalah memeriksa alamat IP melalui terminal dengan menjalankan perintah "ifconfig



Ip address layanan ini adalah 10.0.2.15 dan server sudah aktif dan siap digunakan

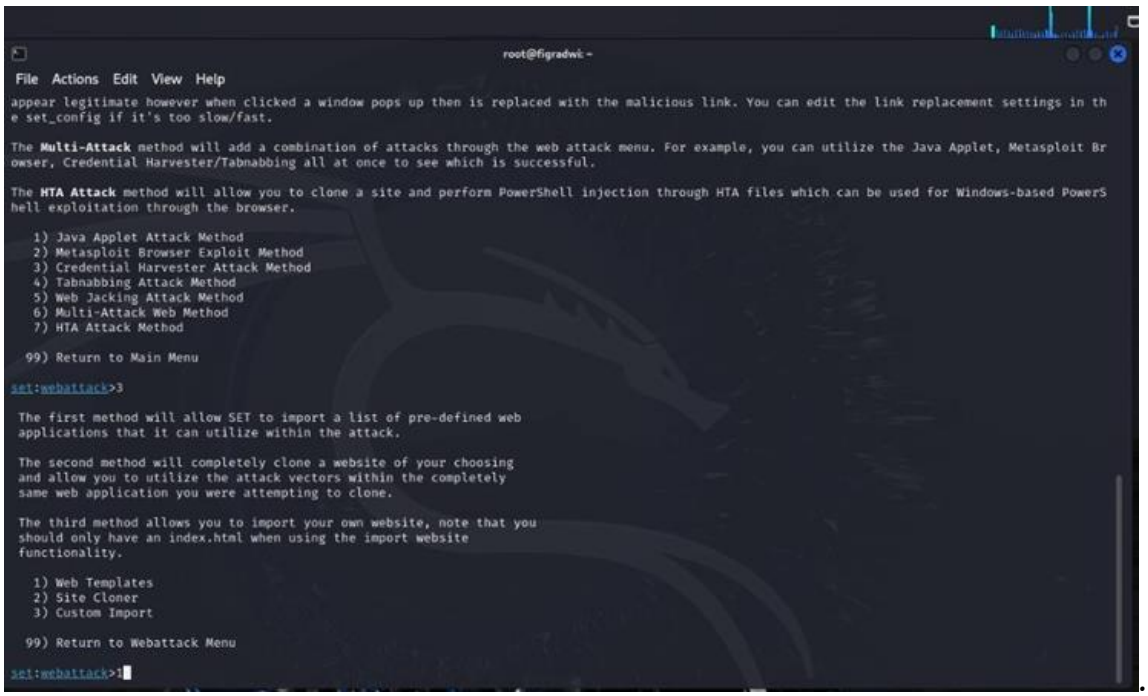
Jalankan SET dengan perintah "setoolkit" lalu ENTER kemudian pilih opsi 1 "Social-Engineering Attacks" dalam phishing digunakan untuk mengumpulkan kredensial login pengguna dengan cara membuat duplikat situs web yang mirip dengan situs asli. Penyerang kemudian membagikan link duplikat tersebut ke target dan menunggu mereka memasukkan kredensial login. Informasi ini kemudian dikumpulkan oleh penyerang untuk tujuan illegal

Selanjutnya pilih opsi 2 "Website Attack Vectors" digunakan untuk menipu pengguna dengan membuat situs web palsu yang mirip dengan situs web asli.

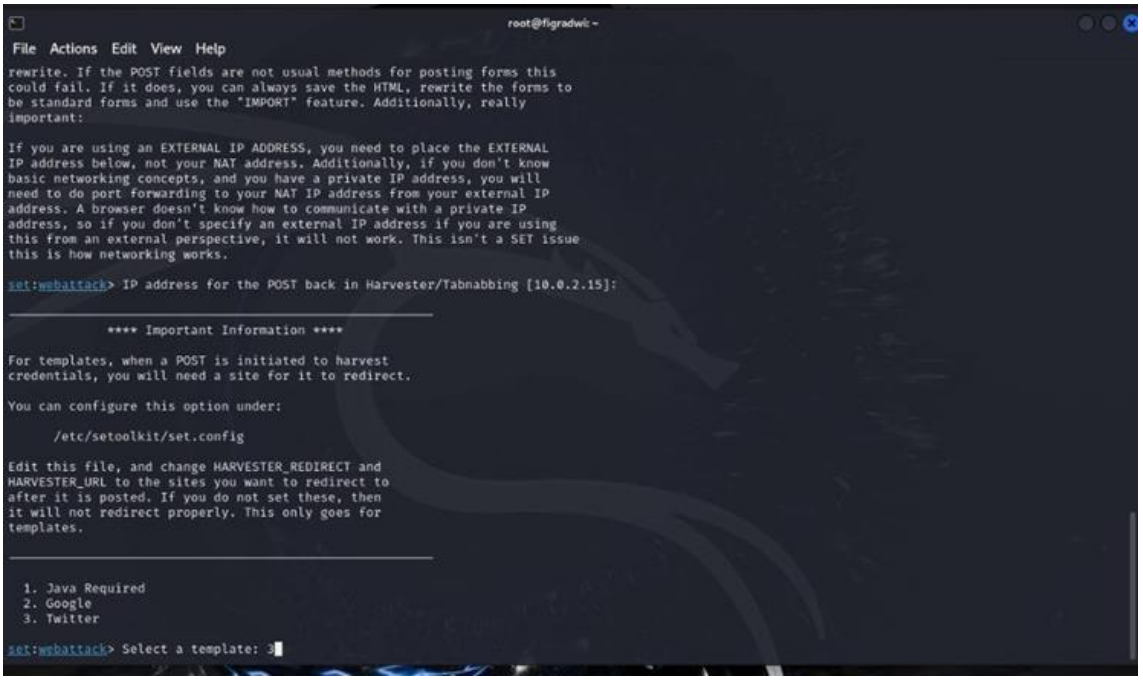


Pilih opsi 3 "Credential Harvestor Attack Method digunakan untuk mencuri kredensial pengguna dengan cara mengkloning situs asli dan menawarkan link yang mirip untuk pengguna. Ketika pengguna mengklik link tersebut dan masuk ke situs yang dikloning, kredensial pengguna akan dikirimkan ke penyerang tanpa mereka menyadari.

Selanjutnya memilih opsi 1 "Web Templates" digunakan untuk membuat situs web palsu yang mirip dengan situs web asli. Pelaku phising menggunakan template untuk menciptakan tampilan yang mirip dengan situs web sah, sehingga korban tidak curiga dan menginputkan informasi sensitif ke situs web palsu.



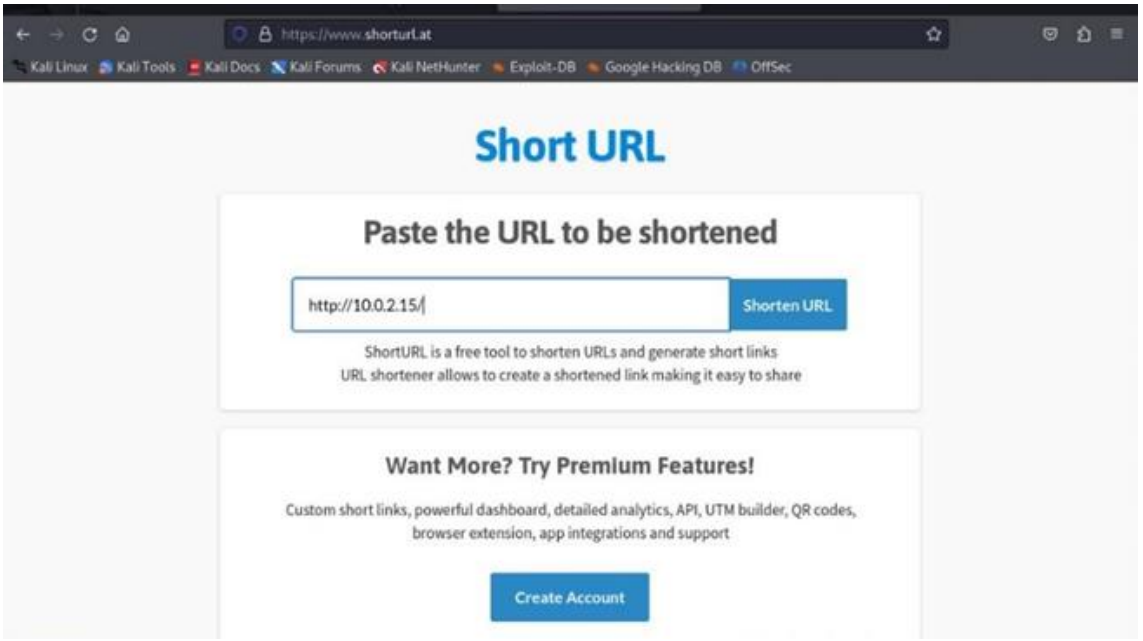
Pilih opsi 3 "TWITTER" yang akan menciptakan tampilan mirip dengan situs web asli



Dan "Dan akan muncul tampilan seperti dibawah ini, sedang mengkloning situs web yang diretas."

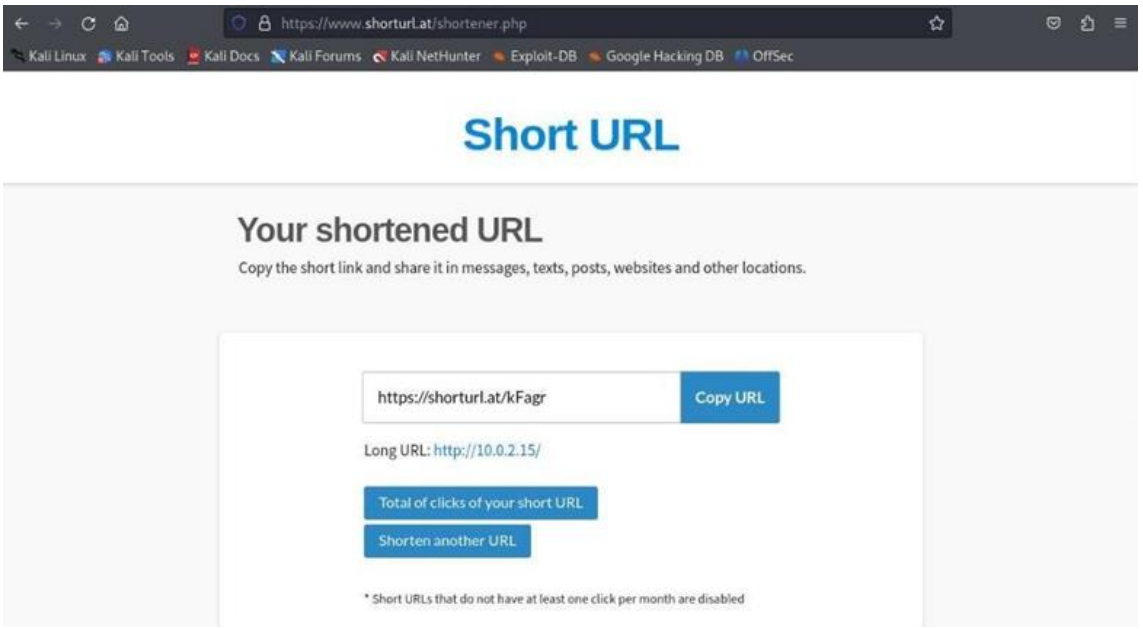
Akses ke Short URL

SHORT URL merupakan aplikasi yang banyak digunakan sebagai media untuk mempermudah pembagian dan pengingatan tautan, terutama tautan yang panjang dapat diakses oleh khalayak umum. Dalam melakukan serangan phisingpada halaman website pendistribusian jaringan lokal harus dilakukan dengan melakukan konfigurasi tunels yang sudah disediakan oleh SHORT URL. Buka laman web layanan SHORT URL lalu masukkan alamat IP yang sebelumnyatelah diverifikasi, dengan menambahkan prefix "http://" seperti pada tampilan di bawah ini.



Selanjutnya, klik tombol "SHORTEN URL" untuk menghasilkan tautan yang lebih ringkas agar mudah dibagikan.

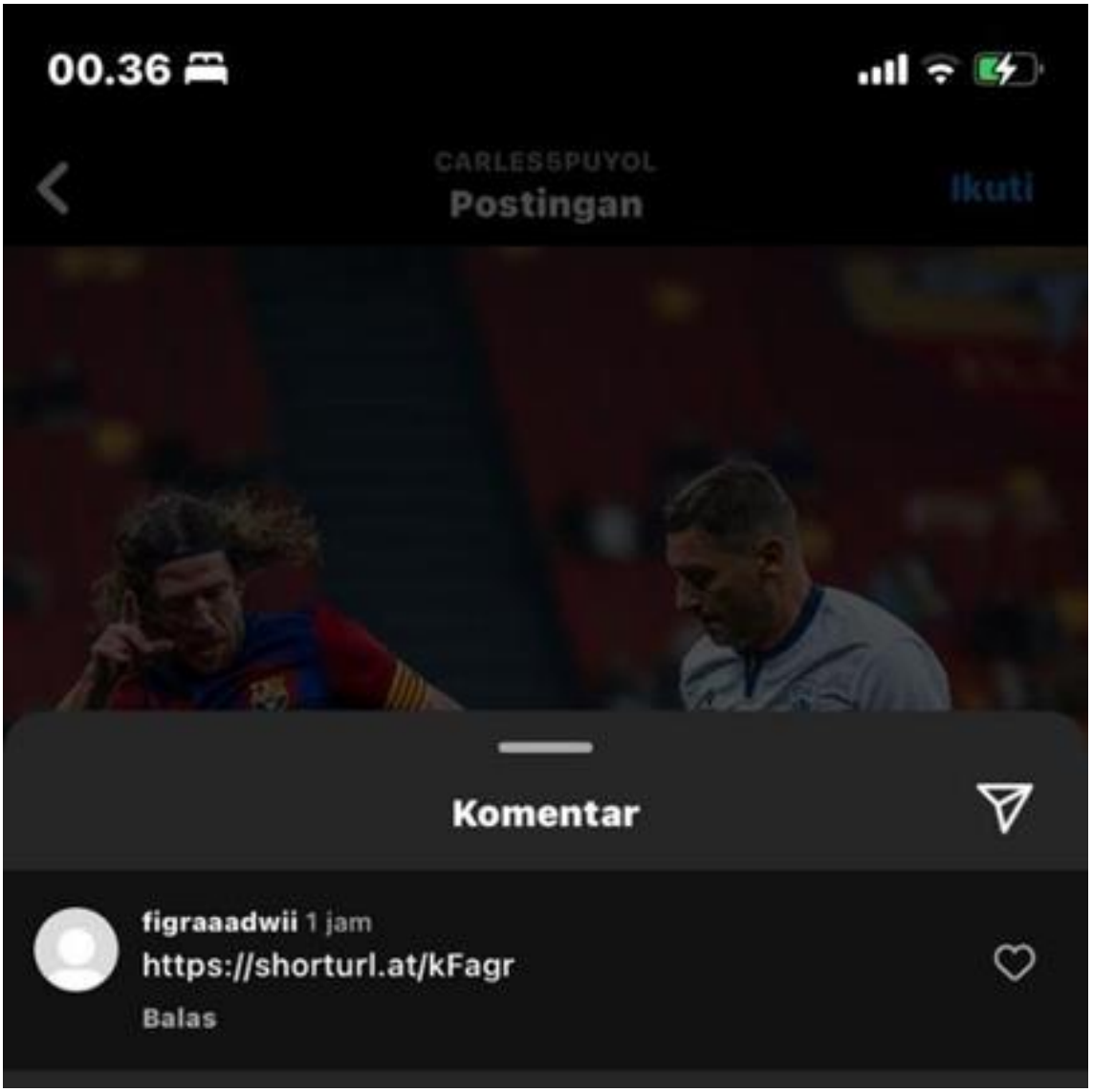
Apabila URL telah diubah seperti tampilan di bawah ini, maka URL tersebut telah berhasil akan digunakan sebagai pendistribusian domain publik ke jaringan lokal pelaku kejahatan dunia maya, sehingga website yang dibuat untuk melakukan phising dapat diakses oleh korban yang dituju.



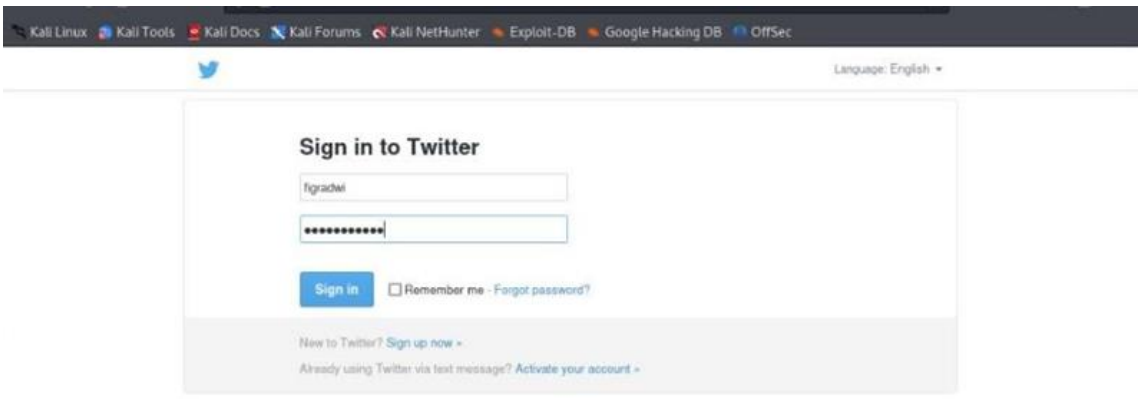
HASIL DAN PEMBAHASAN

Berhasilnya percobaan serangan tersebut menggambarkan bagaimana penyerang dapat melakukan serangan phishing untuk mengumpulkan kredensial login korban. Penyerang berhasil mengirimkan link phishing ke korban, dan saat korban mengakses link tersebut, penyerang dapat mengumpulkan informasi login yang dimasukkan oleh korban. Hal ini membuat akun korban rentan disalahgunakan oleh penyerang.

Ini adalah tampilan bahwa LINK tersebut sudah sampai ke akun pengguna dan siapapun yang melihat akan menelusuri website phising tersebut dan nantinya korban akan mencoba akses websit tersebut, lalu penyerang akan mengumpulkan data keamanan seperti username beserta password korban dan mencatat respons dari platform media sosial.

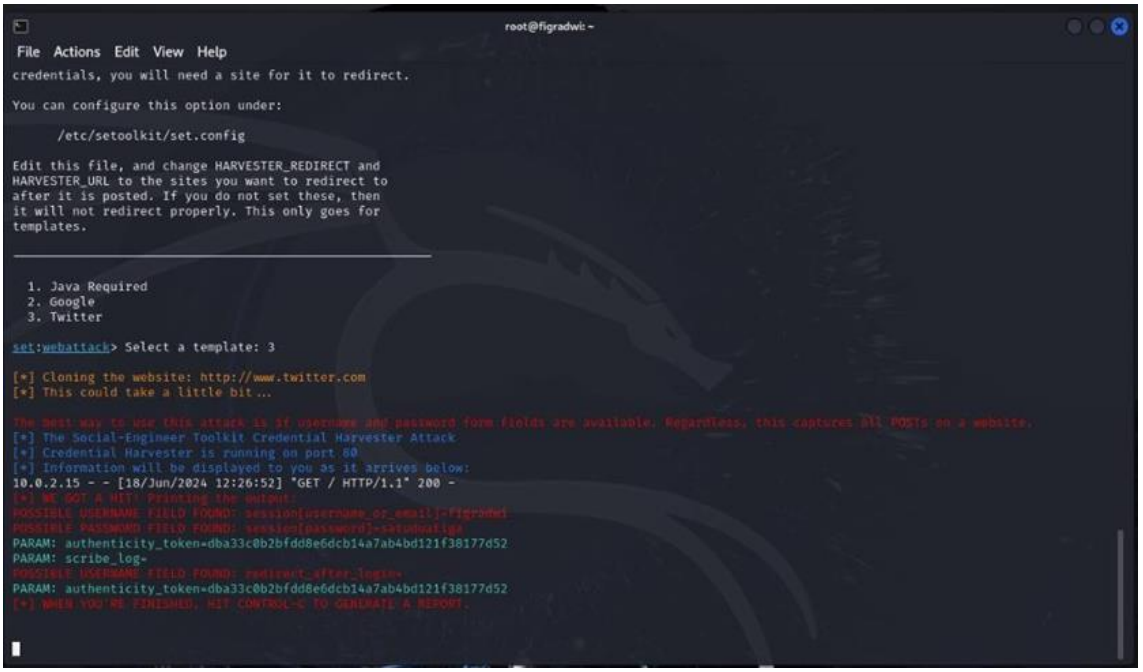


Setelah korban mengklik link tersebut maka akan otomatis terbuka kehalaman cloning website yang telah dilakukan untuk phising dan korban akan melakukan login ke akun yang dimiliki



Namun saat korban telah melakukan login akan dibawa kehalaman lain seakan-akan korban salah memasukan password akun tersebut.

Namun yang sebenarnya terjadi bahwa akun korban telah didapatkan oleh hacker pembuat website phising tersebut.



KESIMPULAN

Dapat disimpulkan bahwa pengguna media sosial perlu memiliki kesadaran yang tinggi akan bahaya serangan phishing dan harus berhati-hati dalam membuka serta mengakses LINK yang diterima, terutama jika LINK tersebut terlihat mencurigakan. Mereka harus selalu memverifikasi sumber LINK atau pesan yang diterima, memastikan bahwa LINK atau pesan tersebut berasal dari sumber yang dapat dipercaya. Media sosial biasanya menyediakan fiturfitur keamanan untuk melindungi akun pengguna, seperti verifikasi dua faktor, dan pengguna harus mengaktifkan serta memanfaatkan fitur-fitur tersebut untuk meningkatkan keamanan akun mereka. Selain itu, pengguna harus rutin memantau aktivitas pada akun media sosial mereka dan segera melaporkan serta mengambil tindakan jika terdapat aktivitas yang mencurigakan.

DAFTAR PUSTAKA

Agustian Akbar, D., Rahdian, M., Kurnia, E., Genggam, R. M., Bintang, S., Purwoko, R., Siber, P., & Negara, S. (2024). Analisis Web Phishing Menggunakan Metode OSCAR Forensic (Studi Kasus: Follower Instagram Gratis). Jurnal Teknik Informatika (JTINFO), 3(1), 18–

24. [2] S. Farizy and E. S. Eriana, *Cloud Computing Komputasi Awan*, no. 1. 2011.

Ariani, P. C., Jayanti, K. S., Atmaja, I. G. B. W., Dewi, I. G. A. A. A., Saskara, G. A. J., & Listartha, I. M. E. (2023). Comparative Analysis of

Phishing Tools on Social Media Sites. Ultimatics: Jurnal Teknik Informatika, 15(1), 22–27. https://doi.org/10.31937/ti.v15i1.2920

Indrajit, P. R. (2016). Keamanan Informasi dan Internet. Yogyakarta: Preinexus

S. Wahyuni, I. M. Raazi, dan D. I. Dwitawati, "Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial

ProfesionalMenggunakan Kombinasi Black Eye dan Setoolkit," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 5, no. 1, hlm. 49–55, Feb 2022, Diakses: Nov 23, 2022. [Daring]. Available:

Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 5(1), 49–55. https://doi.org/10.32672/jnkti.v5i1.3962