UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

Tinjauan Dan Implementasi Clickjacking Dalam Tautan Palsu Untuk Eksplorasi Media Sosial

Oleh:

Achmad Firly Henry Egitha

Yunianita Rahmawati

Progam Studi

Universitas Muhammadiyah Sidoarjo

Juli, 2024

Pendahuluan

Clickjacking, sebagai bentuk serangan siber yang merugikan, mengintegrasikan teknik manipulatif yang memanfaatkan ketidaktahuan pengguna untuk menjalankan klik pada elemen tersembunyi dalam suatu website. Serangan ini memiliki dampak serius, mulai dari potensi pencurian informasi pribadi hingga pelaksanaan tindakan yang tidak dikehendaki oleh pengguna. Tinjauan terhadap clickjacking mendalam pada mekanisme serangan ini menggambarkan kompleksitas dan kemampuannya untuk mengelabui pengguna secara tak terlihat. Implementasi serangan clickjacking melibatkan pemanfaatan teknologi dan strategi yang semakin canggih untuk mengeksploitasi kerentanan di dalam desain dan perilaku pengguna.

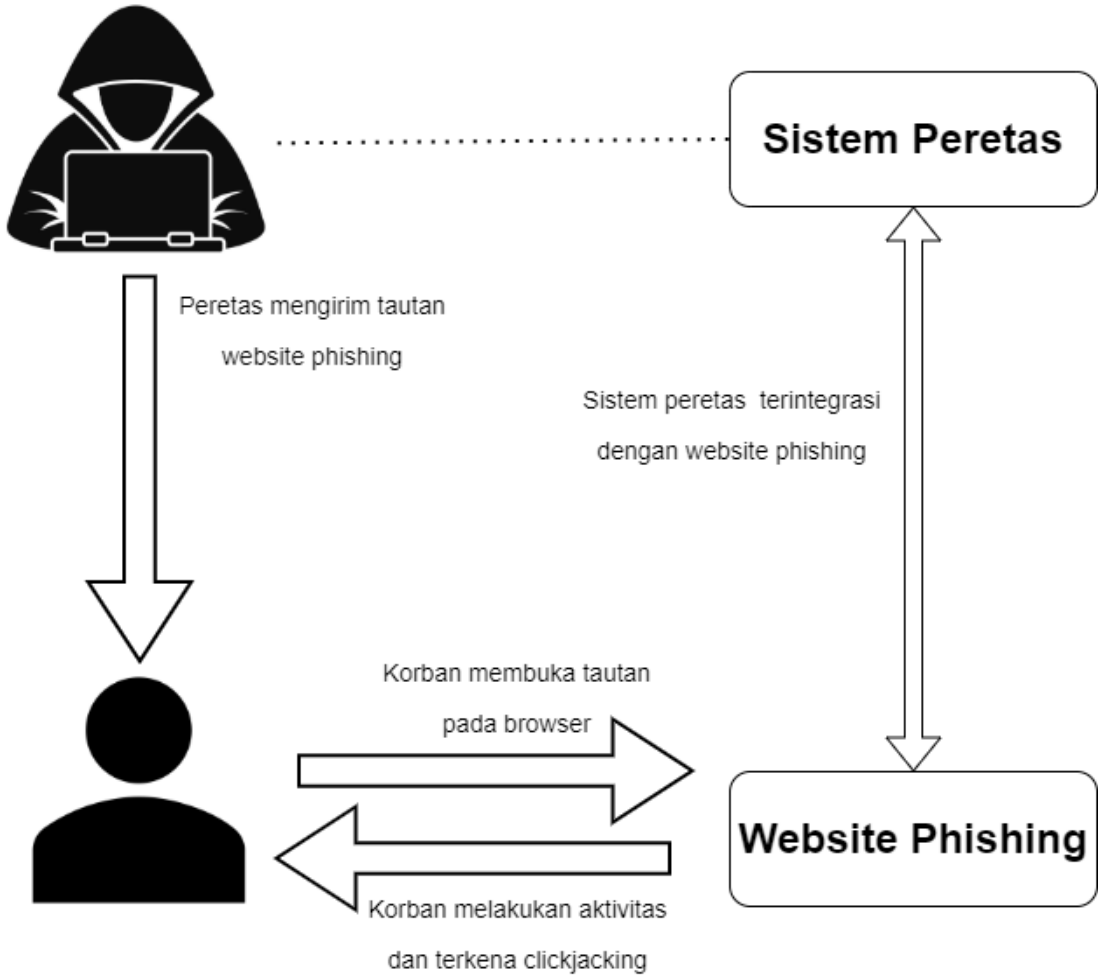
Pertanyaan Penelitian (Rumusan Masalah)

1. Apa saja alat dan bahan yang digunakan dalam serangan tautan palsu?
2. 2. Apa manfaat dari melakukan penelitian terhadap serangan tautan palsu?
3. Bagaimana teknik clickjacking digunakan dalam serangan tautan palsu di media sosial?

4. Bagaimana cara untuk mengetahui lokasi sebuah perangkat denganteknik clickjacking?

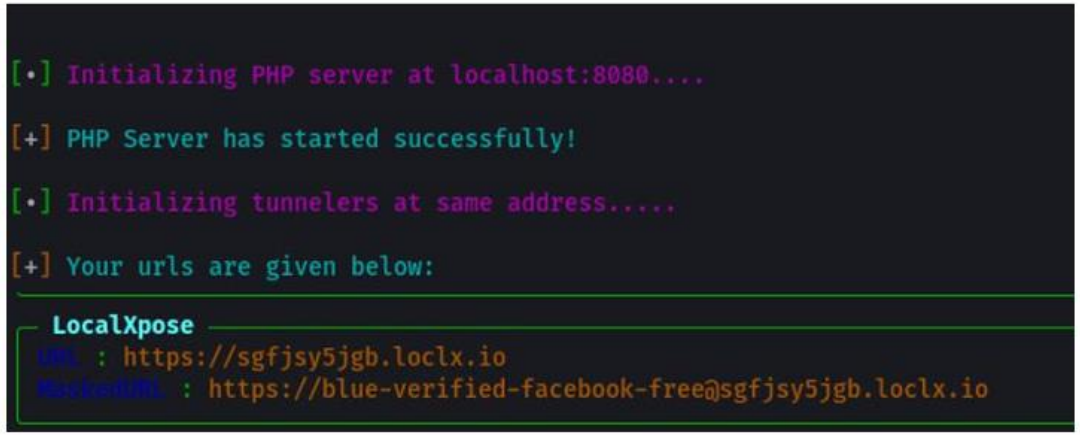
Metode

Metode Clickjacking



Hasil

Hasil Merancang Tautan Dengan Fungsi Clickjacking



Pembahasan

Implementasi serangan clickjacking ini diawali dengan persiapan dan pemahaman terkait alat-alat yang akan digunakan, contoh alat yang digunakan meliputi hardware dan software. Hardware terdiri dari device komputer atau laptop, router wifi dan flashdisk, sedangkan untuk software yang digunakan tools basis sistem operasi linux.

Merancang Tautan

Pada Proses perancangan tautan opsional ini bertujuan untuk memanipulasi aktivitas korban dalam skenario clickjacking, sebuah bentuk serangan di mana pengguna internet secara tidak sadar diarahkan untuk melakukan tindakan tertentu tanpa pengetahuan mereka sendiri.

Pembahasan

Implementasi

Setelah pemilihan tautan sesuai dengan tunel yang telah ditetapkan, langkah selanjutnya melibatkan implementasi pengiriman tautan palsu melalui platform media sosial seperti Facebook. Dalam skenario ini, penyerang menggunakan akun palsu untuk memposting tautan palsu yang menyamar sebagai tautan yang sah atau dapat dipercaya. Tautan disematkan dalam postingan yang menjanjikan konten menarik atau mengecoh, seperti penawaran khusus, konten eksklusif, atau informasi terbaru. Ketika pengguna Facebook melihat postingan tersebut dan tertarik untuk mengeklik tautan, mereka akan dialihkan ke halaman web yang telah dimanipulasi dengan teknik clickjacking.

Pembahasan

Implementasi

Setelah pemilihan tautan sesuai dengan tunel yang telah ditetapkan, langkah selanjutnya melibatkan implementasi pengiriman tautan palsu melalui platform media sosial seperti Facebook. Dalam skenario ini, penyerang menggunakan akun palsu untuk memposting tautan palsu yang menyamar sebagai tautan yang sah atau dapat dipercaya. Tautan disematkan dalam postingan yang menjanjikan konten menarik atau mengecoh, seperti penawaran khusus, konten eksklusif, atau informasi terbaru. Ketika pengguna Facebook melihat postingan tersebut dan tertarik untuk mengeklik tautan, mereka akan dialihkan ke halaman web yang telah dimanipulasi dengan teknik clickjacking.

Analisis Hasil Proses Dibalik aktivitas user pada UI website, peretas telah merecord hasil inputan user dan menyimpan pada direktori peretas. (Hasil data disamarkan).

Temuan Penting Penelitian

Penelitian ini akan dibagi menjadi 4 pokok yaitu rancangan penelitian, pengumpulan data, lingkungan penelitian, analisis data. Penelitian ini akan memanfaatkan sistem operasi kali linux sebagai platform untuk melakukan bentuk serangan siber phishing attack clickjacking. Tools yang digunakan adalah PyPhiser, tools ini bekerja dalam bentuk sistem dengan bahasa python. Tools ini memiliki tujuan untuk mendapatkan informasi dari korban dengan menggunakan tautan palsu. Tautan ini akan mengarah ke website phishing dalam bentuk media sosial.

Manfaat Penelitian

1. Memahami alat dan bahan yang digunakan oleh peretas untuk mengetahui informasi korban dengan teknik clickjacking.
2. Mendapatkan informasi korban dengan memanfaatkan tautan palsu.
3. Menganalisis teknik clickjacking digunakan dalam serangan tautan palsu di platform media sosial.
4. Mengetahui lokasi dari sebuah perangkat dengan memanfaatkan tautan palsu

Referensi

[1] H. Abusaimeh and Y. Alshareef, "Detecting the Phishing Website with the Highest Accuracy," TEM J., vol. 10, no. 2, pp. 947–953, 2021, doi: 10.18421/TEM102-58.

[2] [2] M. Arshey and A. V. K. S, "Security of Web Browser : A Study on Attacks and Their Defences," no. July, 2023.

[3] [3] D. J. Liu, G. G. Geng, X. B. Jin, and W. Wang, "An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment," Comput. Secur., vol. 110, p. 102421, 2021, doi: 10.1016/j.cose.2021.102421.

[4] [4] P. Kalaharsha and B. M. Mehtre, "Detecting Phishing Sites -- An Overview," pp. 1–13, 2021, [Online]. Available: http://arxiv.org/abs/2103.12739

[5] [5] A. O'Mara, I. Alsmadi, and A. Aleroud, "Generative Adverserial Analysis of Phishing Attacks on Static and Dynamic Content of Webpages," 19th IEEE Int. Symp. Parallel Distrib. Process. with Appl. 11th IEEE Int. Conf. Big Data Cloud Comput. 14th IEEE Int. Conf. Soc. Comput. Netw. 11th IEEE Int., pp. 1657–1662, 2021, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00222. [6] [6] S. Agarwal and B. Stock, "First, Do No Harm: Studying the mani


UMSIDA
DARI SINI PENCERAHAN BERSEMI