JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume XII No 2, Desember 2023
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

IMPLEMENTASI CLICKJACKING DALAM SERANGAN TAUTAN PALSU UNTUK EKSPLORASI MEDIA SOSIAL

Achmad Firly Henry Egitha
Jurusan Teknik Informatika
Universitas Muhammadiyah Sidoarjo
Jl. Raya Gelam 250 Candi Sidoarjo
email: achmadfirly2@gmail.com

Abstrak

Sistem komputer merupakan bukan hal baru di era digital saat ini. Keamanan web adalah aspek yang perlu diperhatikan lebih utama pada aspek keamanan web tersebut. Salah satu bentuk serangan keamanan website yaitu phishing, serangan ini memiliki banyak golongannya salah satunya adalah clickjacking. Serangan ini dapat memanipulasi tindakkan pengguna tanpa diketahui oleh korban. Metode pada penelitian ini akan menggunakan tools pada sistem operasi kali linux yang bisa diakses dengan bebas sebagai sarana belajar melakukan bentuk berangan keamanan website. Selain bisa melakukan serangan, penelitiian ini juga akan melakukan analisis dari hasil serangan dalam bentuk data. Hasil dari penelitian ini adalah pencurian data korban seperti lokasi, nomor seluler dan lain-lain. Kesimpulan dari penelitian ini adalah untuk implementasi clickjcking dalam serangan tautan palsu untuk mendapatkan informasi korban.

Kata Kunci: Peretas, tautan, serangan, klik, pembajakan

1. Pendahuluan

Dalam era saat ini sebuah teknologi menjadi sebuah alat untuk membantu kehidupan sehari-hari. Dengan adanya teknologi manusia dengan mudahnya melakukan apapun yang ingin dilakukan. Penggunaan website sebagai media digital menjadi peringkat 3 besar bagi pengguna sistem informasi online. Namun seiring dengan penggunaan yang pesat, sebuah ancaman terhadap kemanan website juga semakin bermacam-macam. Serangan clickjacking merupakan serangan yang memfokuskan dalam memanipulasi tindakan korban untuk melakukan tindakan yang seharusnya tidak dilakukan oleh korban. Tindakan ini tidak diketahui oleh korban dikarenakan dalam persiapannya sudah disusun rapi sehingga korban kesulitan dalam membedakan antara tautan asli dengan tautan palsu.

Serangan clickjacking menjadi masalah serius dikarenakan merusak data pribadi korban dan bisa disalah gunakan untuk tindakan melawan hukum. Serangan pada penelitian ini bekerja dalam bentuk media sosial dengan memanfaatkan menu login sebagai user interface. Hasil dari login korban akan disimpan pada sistem phising sehingga peneliti sekaligus peretas bisa mengetahui username dan password korban.

Penelitian ini akan menggunakan eksplorasi pendekatan dengan menggunakan tools pada sistem operasi kali linux untuk merancang sebuah serangan keamanan website dengan teknik clickjacking dalam bentuk media sosial. Pada penelitian ini, peneliti akan melakukan perancangan, serangan dan analisis pada teknik clickjacking. Kesimpulan dari serangan ini diharapkan dapat memberikan wawasan dan panduan cara kerja seorang peretas melakukan serangan clickjacking pada website dalam bentuk tautan palsu media sosial.

2. Landasan Teori

Keamanan Web (Web Security)

Keamanan sebuah website merupakan prioritas dalam pengembangan website. Upaya dalam melindungi data pengguna menjadi hal mutlak dan tanggung jawab bagi pengembang perangkat lunak. Sistem kemanan akan terus dikembangkan seiring dengan banyaknya jenis serangan yang terjadi, contohnya serangan sistem keamanan web dalam bentuk tautan palsu. Ini juga mencakup sebuah keamanan dari serangan clickjacking. Tautan palsu yang akan mengarahkan pengguna menuju halaman berbahaya yang terindex oleh elemen clickjakcing.

Human-Computer Interaction (HCI):

Hubungan interaksi manusia dan komputer adalah tujuan utama dari terciptanya user interface yang efisien dan informatif. Pengembangan user interface yang melibatkan teks, gambar dan vidio yang mudah dipahami oleh pengguna menjadi tantangan bagi web developer. Tidak menuntut kemungkinan webite yang sudah terbagun dengan sebaik-baiknya bisa jadi terinstall elemen yang seharusnya tidak ada dalam user interface tersebut. Adanya elemen negatif bisa terjadi karena adanya ulah oknum yang tidak bertanggung jawab atas aksi dan tindakan yang

melanggar etika dan hukum. Sering terjadi website terdeteksi sebuah elemen clickjacking dengan tujuan untuk mengetahui data pengguna yang sifatnya privacy.

Teknik Penipuan (Deception Techniques)

Teknik penipuan dalam konteks seranngan keamanan website menjadi tantangan bagi web developer. Taktik serangan yang sering terjadi pada website ialah phishing. Phishing bisa diakses melalui tautan palsu. Tautan palsu akan mengarahkan pengguna menuju halaman phishing. Disaat pengguna melakukan tindakan klik pada tautan palsu tetrsebut secara tidak disadari pengguna sudah terkena serangan clickjacking. Data yang diinput akan tersimpan pada sistem peretas tanpa diketahui oleh pihak pengguna dan pihak web developer, hal ini terjadi karena pembuatan tautan palsu yang sengaja dibuat dengan kemiripan dengan tautan asli sebesar hampir 100% sehingga manjadi kesulitan dalam menbedakan antara tautan asli dengan tautan palsu.

3. Metode Penelitian

Rancangan Penelitian Forensik

Penelitian ini akan menggunakan dua rancangan penelitian yang pertama ialah rancangan penelitian analisis forensik, rancangan penelitian ini bertujuan untuk menganalisis dan menyelidiki kasus-kasus serangan clickjacking yang sudah ada sebelumnnya seperti kasus kasus undangan online dengan format PDF ataupun Apk. Dalam penelitian ini akan dibahas bagaimana cara peretas melakukan aksinya sehingga mendapatkan data dari korban tanpa diketahui oleh korban itu sendiri.

Penelitian ini akan dimulai dengan menidentifikasi insiden clickjacking yang telah terjadi dan mengumpulkan bukti digital yang relevan, seperti data statistik kasus serangan clickjacking dalam bentuk tautan palsu. Setelah data diperoleh akan dilakukan analisis secara menyeluruh untuk untuk mengetahui teknik serangan yang sering digunakan. Metode yang digunakan clickjacking positif dengan batasan untuk mendapatkan data informasi korban.

Rancangan Penelitian Eksperimental

Rancangan penelitian yang ke dua ini adalah rancangan penelitian eksperimental, sesuai dengan namanya peneliti akan melakukan pengujian clickjacking dengan menciptakan skenario serangan di lingkkungan kendali penuh oleh peneliti. Peneliti akan merancang tautan palsu yang telah di manipulasi agar korban percaya jika tautan tersebut aman untuk di click. Jika tautan telah di click maka korban akan mengirimkan data informasi perangkat yang digunakan namun dengan tampilan media sosial palsu untuk melakukan tindakan bagikan lokasi agar data lokasi korban diserap oleh tautan palsu tersebut. Selama pengujian ini peneliti melakukan monitoring terhadap aktivitas korban, merekam data dan menganalisis data yanng telah diperoleh.

Lingkungan Penelitian

Pada penelitian eksperimental penggunaan teknik clickjacking ini peneliti memilih untuk menggunakan menu prompt pada sistem operasi linux. Peneliti merancang dan mendesain tampilan sosial media palsu agar sesuai dengan tampilan sosial media aslinya. Tujuan dari rancanngan ini untuk menciptakan serangan clickjacking dalam bentuk website phishing dengan tampilan medis sosial.

Sistem Operasi

Peneliti menggunakan sistem operasi Kali Linux sebagai sistem operasi penelitian. Kali Linux adalah distribusi Linux yang populer di kalangan peneliti keamanan dan ethical hacker karena dilengkapi dengan berbagai alat keamanan dan forensik yang berguna.

Analisis Clickjacking

Clickjacking merupakan serangan keamanan yang mengelabuhi korban untuk melakukan tindakan yang tidak disadari oleh korban tersebut. Korban akan membagikan informasi melewati elemen yang sudah dirancang seolah-olah ketika di klik bersifat aman jika dilakukan. Clickjacking termasuk tindakan pencurian data informasi pribadi, penganbilan akun dan penyebaran konten berbahaya.

Teknik Clickjacking

Clikjacking merupakan teknik serangan keamanan yang memanfaatkan teknik penipuan User Interface. Dalam kasus serangan clickjakcing, peretas bisa membuat elemen dengan fungsi untuk menampung informasi dari tindakan korban.

Dampak Serangan

Serangan keamanan dengan teknik clickjakcing memiliki dampak yang merugikan, dalam konteks media sosial, clickjacking dapat mengduplikasi tampilan media sosial tersebut dengan menyisipkan elemen yang tidak seharusnya ada pada media sosial tersebut. Hal ini bisa membuat korban membagikan informasi tanpa harus diketahui oleh pihak pengembang perangkat lunak.

Perlindungan

Untuk melindungi dari dari serangan clickkjacking, perusahaan web dan pengembang perangkat lunak harus memiliki mekanisme dalam aspek keamanan data pengguna. Data dengan sistem keamanan yang baik menjadi faktor penting agar terlindung dari serangan clickjacking.

Kesadaran

Kesadaran pengguna media digital menjadi faktor utama dalam mengatasi serangan clickjakcing. Pengguna harus lebih selektif dan bijak dalam melakukan tindakan dimedia sosial lebih bagi yang membagikan sebuah tautan (LINK).

Hasil Data Forensik

Indonesia tahun 2022 menemukan 164.131 kasus email phishing. Email phishing merupakan modus peretasan dengan menyamar sebagai orang atau organisasi berwenang melalui surat elektronik, dilansir dari DataIndonesia, Rabu (29/2/2023), Badan Siber dan Sandi Negara (BSSN) melaporkan ada 164.131 kasus email phishing di Indonesia pada 2022. Jumlah tersebut paling banyak berasal dari email pribadi, yakni 59.210 kasus. Sebanyak 52.744 kasus email phising berasal dari email grup. Kemudian, ada 52.177 kasus phising yang berasal dari email lainnya. Adapun, 93.897 kasus email phising terjadi saat jam kerja atau pukul 09.00-17.00 Sementara, 70.234 kasus lainnya dilakukan di luar jam kerja pada pukul 17.00 hingga 09.00 [12].

Email phising yang terjadi pada 2022 juga kerap melampirkan sebuah file. Format file yang paling mendominasi memiliki ekstensi .pdf, yakni lebih dari 100.000 kasus. Indonesia menjadi negara kelima terbanyak mengalami kebocoran data. Berdasarkan laporan perusahaan keamanan siber asal Belanda, Surfshark menunjukkan, ada 5,34 miliar akun yang mengalami kebocoran data secara global sepanjang 2022. Dari jumlah itu, kasus kebocoran terbanyak terjadi di Rusia yang mencapai 103,49 juta akun sepanjang 2022. Posisi kedua ditempati oleh China dengan 33,88 juta akun yang dilaporkan mengalami kebocoran data. Kemudian, ada 22,37 juta akun yang mengalami kebocoran data di Amerika Serikat. Sebanyak 19,77 juta akun juga mengalami kebocoran data di Prancis. Indonesia berada di posisi kelima dengan 14,66 juta akun yang datanya bocor [12].

Hasil Data Eksperimental

Data eksperimental dilakukan dengan cara melakukan implementasi tindakan serangan phishing secara langsung oleh peneliti, peneliti membuat tautan palsu dengan menggunakan tools phishing website, setelah tautan siap untuk disebar pada sosial media, peneliti mencoba pada pada salah satu media sosial whatsapp dan dikirim pada sebuah grup dengan jumlah 202 anggota, penelitian ini dilakukan selama kurang lebih 73 jam atau sekitar 3 hari. Setelah data didapatkan peneliti mendapatkan hasil dari 202 anggota terdapat 89 anggota telah klik tautan phishing tersebut, 89 anggota tersebut terdiri dari 17 telah aktif GPS dan 3 anggota menggunakan Dekstop 86 mengunakan mobile android.

4. Kesimpulan

Kesimpulan dari penelitian ini adalah pemahaman terkait teknik clickjacking dengan memanfaatkan tools pada sistem operasi kali linux, namun perlu digaris bawahi jika penelitian ini dilakukan dengan kendali penuh oleh peneliti sehingga data yang diperoleh tidak di salah gunakan dan penelitian ini tidak direkomendasikan bagi oknum yang tidak baik. Penelitian menjadi bukti jika sebuah kemanan website perlu ditingkatkan untuk menghindari dari serangan phishing dengan teknik clickjakcing dalam bentuk tautan palsu media sosial. Saran peneliti jika ingin menggunakan sebuah layanan media sosial baiknya menggunakan halaman resmi dari website terkait guna menghindari aksi kejahatan clickjacking.

6. Daftar Pustaka

[1] 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.

[2] A. SankaraNarayanan, “Clickjacking Vulnerability and Countermeasures,” *Int. J. Appl. Inf. Syst.*, vol. 4, no. 7, pp. 7–10, 2012, doi: 10.5120/ijais12-450793.

[3] L. S. Huang, A. Moshchuk, H. J. Wang, S. Schechter, and C. Jackson, “Clickjacking: Attacks and defenses,” *Proc. 21st USENIX Secur. Symp.*, pp. 413–428, 2012.

[4] K. Puneet, “IRJET- A Review on Clickjacking Attack and its Defense Mechanism,” *Irjet*, vol. 8, no. 4, pp. 1098–1101, 2021.

[5] I. Processing, “Available on : Elsevier-SSRN Phishing Attack Detection using Feature Selection Techniques,” pp. 1–7, 2019.

[6] R. Hakimi, “Jurnal Pustakawan Indonesia Volume 11 No. 2 Studi Isu Keamanan Jaringan Pada Facebook Rifqy Hakimi 1 1,” vol. 11, no. 2, pp. 1–14.

[7] 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.

[8] R. Damodaram, "Study on Phishing Attacks and Antiphishing Tools," *Int. Res. J. Eng. Technol.*, vol. 3, no. 1, pp. 700–705, 2016.
[9] A. Perdananto, "Sistem Pelacak Menggunakan GPS Tracker Untuk Ponsel Android," *J. ICT Akad. Telkom Jakarta*, vol. 8, no. 15, pp. 59–63, 2017.
[10] 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.
[11] E. Dodsworth, "63 cartographic perspectives Mapping: Methods & Tips Historical Mapping Using Google Earth," no. 61, pp. 63–69, 2008, [Online]. Available: http://www.davidrumsey.com/.
[12] Keamanan Siber Indonesia 2022.