ISSN: 2745-375 **Djtechno : Journal of Information Technology Research**
Vol. 2, No. 1 Juli Tahun 2021

ANALISIS KEAMANAN INFORMASI PENGGUNA MEDIA SOSIAL MENGGUNAKAN SETOOLKIT MELALUI TEKNIK PHISING

Malahayati[1)], Darul Fata[2)]
1)Program Studi Teknologi Informasi , Fakultas Sains & Teknologi,Universitas Islam Negeri Ar-Raniry, Indonesia

E-mail: fatadarul@gmail.com

Abstrak

Salah satu perkembangan teknologi itu yaitu berupa Perkembangan jejaring media sosial. Banyak kemudahan yang ditawarkan oleh media komunikasi baru ini, pengguna jejaring sosial dapat menyebarkan maupun mencari pesan atau informasi dengan cepat. Meningkatnya penggunaan jejaring sosial di indonesia disebabkan oleh semakin lengkapnya fasilitas akses internet. Kita tidak mengetahui apakah aplikasi media sosial ini aman untuk digunakan, karena dunia internet tentu tidak lepas dari masalah keamanan karena di internet data bisa masuk ke mana saja. Oleh karena itu, disarankan kepada setiap user untuk tetap memperhatikan keamanan informasi dalam menggunakan social media.

Kata kunci : Media Sosial, Phising

Abstract

One of the technological developments is the development of social media networks. Many of the conveniences offered by this new communication media, social network users can spread or search for messages or information quickly. The increasing use of social networks in Indonesia is due to the increasingly complete internet access facilities. We do not know whether this social media application is safe to use, because the world of the internet certainly cannot be separated from security problems because on the internet data can go anywhere. Because of that, it is advisable for every user to pay attention to information security when using social media.

Keywords: Social Media, Phishing

PENDAHULUAN

Perkembangan teknologi informasi semakin mempengaruhi kehidupan manusia. Segala aspek kehidupan telah mengandung unsur internet dalam memudahkan pekerjaan. Kata teknologi da internet tak asing lagi di kalangan masyarakat bahkan pada masyarakat awam sekalipun. Hal ini didasari telah menyebar luasnya koneksi internet dan sangat mudah untuk diakses. Perkembangan teknologi sejauh ini sangatlah pesat terutama pada bagian internet yang dapat di manfaatkan untuk komunikasi tidak hanya bia digunakan pada perengkat besar seperti personal computer atau laptop yang terhubung lewat jaringan web akan tetapi penggunaan pada bidang komunikasi saat ini bisa di akses lewat perangkat yang lebih ringkas yaitu mobile.pesatnya perkembangan teknologi pda mobile ini sekarang dapat digunakan tidak sekedar untuk komunikasi tapi kita dapat mengakses berbagai macam aplikasi yang sudah saling terhubung di internet diantaranya ada fintech, game online, aplikasi belanja, akses map, aplikasi bank, streaming video dan music, aplikasi Kesehatan dan bahkan aplikasi kencan semua kini dapat di akases hanya melalui mobile. terdapat sangat banyak aplikasi yang mendukung kemudahan komunikasi maka terciptalah media sosial. Media sosial itu sendiri pun tergolong dalam beberapa bidang dalam mampublikasikan konten dan kuminaksi, ada media sosial chat yang mendukung penuh untuk melakukan chatingan dan juga ada media sosial share yang mendukung untuk melakukan publish text, gambar , dan video untuk di sebarluaskan dan dapat di akses oleh seluruh pengguna lainnya.

Menurut data statistic dari hootsuite pengguna media sosial di dunia mencapai 3,8 miliar orang dari jumlah populasi dunia yaitu 7,75 miliar. Di Indonesia sendiri pengguna media sosial mencapai 160 juta orang dari jumlah populasi 272 juta orang. Disini terbukti bahwa orang menggunakan media sosial untuk tetap terhubung satu sam alain dan angka tersbut akan bertambah setiap tahunnya.

Disamping berbagai macam manfaat dari perkembangan teknologi terutama pada media sosial yang bisa membuat kita tetap terhubung bahkan dengan orang

yang jaraknya cukup jauh sekalipun, pasti akan tetap terdapat kerugian berupa ancaman yang dapat menganggu kenyamanan pengguna dan juga menyalahgunakan pemanfaatan media sosial ini. Pada kesempatan ini penulis akan mengangkat satu kategori dari media sosial yaitu media sosial share yang termasuk di dalamnya facebook, twitter, dan Instagram untuk melakukan testing kloning halaman melakukan teknik phising sehingga penulis memberi judul pada makalah ini "Analisis Keamanan Informasi Pengguna Media sosial Menggunakan setolkit melalui Teknik phising"

Dari latar belakang di atas dapat dirumuskan satu permasalahan "bisakah laman media sosial di kloning menggunakan teknik phising pada sistem login"

Tujuan dari penelitian ini adalah melakukan testing terhadap halaman media sosial untuk mengetahui apakah media sosial tersebut dapat di kloning sehingga dapat menimbulkan pencurin data pada saat melakukan login maka dilakukan testing menggunakan setoolkit.

Media sosial adalah media online yang mendukung setiap individu untuk saling terhubung dengan pengguna lain untuk berpartisipasi, berinteraksi, dan berbagi dengan media sosial pengguna dapat dengan mudah menyebar luaskan konten. Media sosial terdapat beberapa ketegori diantaranya: media sosial share, media sosial publish,dan media sosial chat. Seiiring perkembangan teknologi kini pengguna media sosial semakin bertambah banyak. (Paramitha, 2011)

Seiring perkembangan teknologi maka makna dari media sosial dan perannya semakin tumbuh pesat. Saat ini, media sosial dapat diakses dengan mudahnya melalui mobile. Dampak tersebut juga mulai secara perlahan menggantikan media massa konvensional (TV, majalah, koran, radio) dalam konteks menyebarkan berita dan informasi.

Phising adalah upaya utuk mendapatkan informasi dengan teknik pengelabuan. Data yang di phising merupakan data prbadi yang di input oleh korban pada laman palsu yang di kloning dari laman tertentu. Kegiatan phising memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Pelaku

phising menampakkan diri sebagai pihak berwenang dengan menggunakan website atau email palsu yang tampak meyakinkan dan kemudian setelah informasi diperoleh akan digunakan dengan tuuan kejahatan. Jenis-jenis phising diantaranya : emil phising, spear phising, whaling, dan web phising. (Kurniawan, Suryadi. 2020)

Phising sendiri terbagi menjadi beberapa jenis dan teknik yang sering digunakan oleh penjahat cyber. Adapun diantaranya :

- Spear Phising
  Mengirim email secara secara langsung kepada target dan mengaku sebagai pihak resmi yang terpercaya.
- Deceptive Phising
  Mengaku sebagai pihak resmi yang meminta verifikasi akun, mengubah kata sandi, melakukan pembayaran, dan hal sejenis lainnya yang bersangkutan dengan pelayanan sebagai pihak resmi.
- Web phising
  Upaya memanfaatkan website palsu atau kloning untuk mengelabui target. Web hasil kloning tersebut akan terlihat mirip dengan web resmi dengan menggunakan domain yang mirip.

METODE PENELITIAN

Adapun metode penelitian yang digunakan melalui studi literature dan percobaan, yang bertujuan mendapat pengetahuan. Studi literature didapatkan melalui jurnal, internet, dan sebagainya. Sedangkan percobaan dilakukan sendiri dengan menggunakan sistem operasi kali linux dan tool setoolkit dan menerapkan teknik phising.

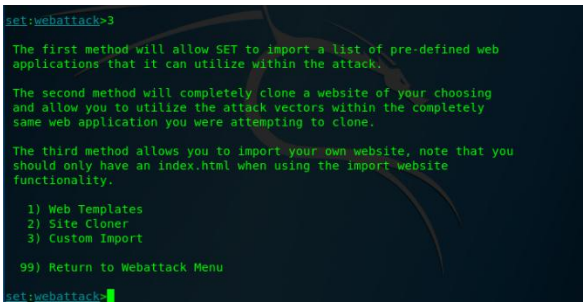
HASIL DAN PEMBAHASAN

1.1 Teknik Phising

Cara kerja phising disini dengan memanipulasi dan memanfaatkan kelalaian korban. Pada pengetesan ini menggunakan teknik web phising dengan memanfaatkan laman login pada media sosial. Target dari phising adalah informasi pribadi yang berupa username dan password pengguna dan dimanfaatkan untuk mengusai akun korban. Apabila web phising berhasil maka data yang didapat akan dimanfaatkan untuk kejahatan diantaranya:

- Menjual informasi yang didapatkan
- Menggunakan sebagai kepentingan politik
- Melakukan aksi penipuan
- Membobol akun yang terverifikasi lainnya dengan menggunakan data yang dimiliki
- Melakukan pinjaman online mengatasnamakan korban

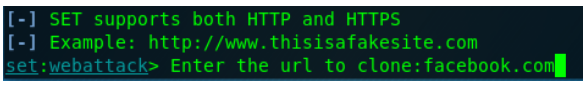
Pada testing kali ini menggunakan setoolkit pada kali linux yang merupakan phising tingkat dasar yang berupa kloning website melalui website resmi.



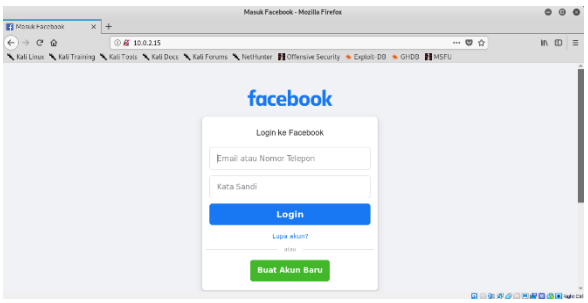
Karena mengkloning website yang sudah ada maka kita memilih site cloner pda setoolkit. Disini kita akan mengset web yang akan digunakan. Website yang akan digunakan adalah facebook, twitter, dan instagram

1.2 Implementasi Teknik Phising Pada Facebook

Pada menu site cloner di tool setoollkit akan dimintakan url web yang akan di kloning pada bagian set webattack. Disini kita akan memasukkan target implementasian yang pertama yaitu facebook.com.



Hasil dari pengkloningan dari url facebook.com akan menghasilkan halaman web utama yang persis dengan facebook yang diakses dengan ip address pelaku phising. Dikarenakan kali linux diakases melalui virtualbox maka jaringan yang digunakan adalah jaringan kabel dari jaringan yang terdapat pada sistem operasi utama sehingga menghasilkan ip address 10.0.2.15. Ip address tersebut digunakan untuk mengakses halaman hasil kloning.



Terlihat halman web hasil kloning melalui setoolkit dengan teknik phsising. Hasil ini adalah teknik phising dasar yang hanya dapat diakses melalui satu jaringan saja.karena halaman web hasil kloning sama persis dengan web resmi mka dapat

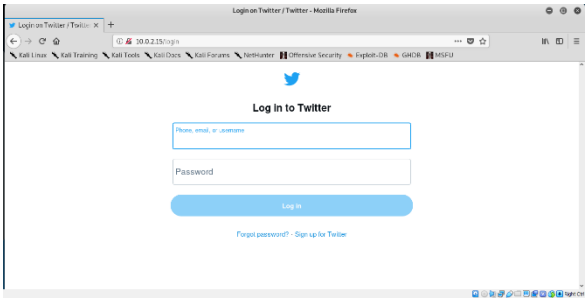
mengelabui korban untuk melakukan login di halaman tersebut dan setelah login maka halaman tersebut akan mengarah ke web yang asli untuk melakukan login ulang dan proses phising pun selesai. Hasil informasi yang di sertakan dalam halaman login akan terdeteksi otomatis pada terminal pelaku. Hal ini membuktikan bahwa hasil testing mengkloning halaman facebook dengan teknik phising berhasil. Karena menggunkan teknik phsiing tingkat dasar maka yang bisa mengakses laman tersebut hanya yang tersambung dalam satu jaringan dan sangat mudah membedakan url phising dengan yang aslinya akan tetapi praktek teknik phising ini dapat ditingkatkan dan dibuat menyerupai url asli yang sudah tersebar luas dan sangat sulit untuk dibedakan.

1.3 Implementasi Teknik Phising Pada Twitter

Pada target selanjutnya yaitu twitter juga menggunakan cara yang sama dalam pengimplementasian teknik phising ini.

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:twitter.com
```

Pada menu site cloner sertakan url target pada bgian set web attack dan kemudian akan dihasilkan halaman web kloning yang di akses melalui ip address.



Maka terlihat halaman web hasil kloning yang juga sama persis dengan halaman asli. Hal ini membuktikan bahwa twitter juga dapat di kloning menggunakan Teknik phising. Karena menggunkan teknik phsiing tingkat dasar maka yang bisa mengakses laman tersebut hanya yang tersambung dalam satu jaringan dan sangat mudah membedakan url phising dengan yang aslinya akan tetapi praktek teknik phising ini dapat ditingkatkan dan dibuat menyerupai url asli yang sudah tersebar luas dan sangat sulit untuk dibedakan.

1.4 Implementasi Teknik Phising Pada Instagram

Target selanjutnya adalah Instagram, masih menggunakan cara yang sama pada teknik phising dengan memasukkan url target yaitu Instagram.com pada menu site cloner di bagian set web attack.

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:instagram.com
```

Maka akan menghasilkan web kloning yang di akses melalui ip address pada peramban. Karena menggunkan teknik phising dasar halaman tersebut hanya

Maka kloning web Instagram terbukti berhasil dengan menghasilkan web yang mnyerupai web resmi yang dapat mengelabui korban. Jadi, teknik phisng uga bisa di implementasikan terhadap Instagram dan juga berbagai media sosial lainnya. Dengan teknik phising yang lebih lanjut makan akan menghasilkan url yang menyerupai url asli yang sulit untuk dibedakan. Hal ini membuktikan bahwa media sosial rentan terhadap teknik phising yang menghasilkan kloning halaman web di sistem login media sosial.

KESIMPULAN

Media sosial adalah media online yang mendukung setiap individu untuk saling terhubung dengan pengguna lain untuk berpartisipasi, berinteraksi, dan berbagi dengan media sosial pengguna dapat dengan mudah menyebar luaskan konten.

Phising adalah upaya utuk mendapatkan informasi dengan teknik pengelabuan. Data yang di phising merupakan data prbadi yang di input oleh korban pada laman palsu yang di kloning dari laman tertentu. Kegiatan phising memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Pelaku phising menampakkan diri sebagai pihak berwenang dengan menggunakan website atau email palsu yang tampak meyakinkan dan kemudian setelah informasi diperoleh akan digunakan dengan tuuan kejahatan.

Hasil percobaan membuktikan bahwa semua media sosial rentan terhadap teknik phising. Berbagai halaman bisa saja di cloning untuk mengelabui pengguna. Aksi phising ini sangat sering terjadi maka dihibau kepada seluruh pengguna media sosial agar berhati-hati dan selalu memperhatikan url saat mengakses laman tertentu.

Adapun kiat-kiat yang dapat dilakukan untuk bisa terhindar dari kejahatan phising :

- Selalu update informasi mengenai phising

  Tidak menutup kemungkinan jenis kejahatan online terutama phising akan terus berkembang
- Perhatikan link yang diterima, jangan asal klik

  Pelaku biasanya mengirim link phissing melalui email ataupun sms, perhatikan link tersebut terlebih dahulu. Selalu ada hal yang membedakan link resmi dengan yang palsu.
- Pastikan kemanan website saat mengakses

  Jangan kunungi website yang tidak aman, lakukan trnsaksi pada yang menggunakan SSL yaitu web yang ditandai protocol HTTPS
- Update selalu peremban atau browser
- Berhati-hati dan waspada saat diminta data pribadi
- Gunakan verifikasi 2 langkah pada sistem login media sosial

DAFTAR PUSTAKA

Abdul Halim Barkatullah dan Teguh Prasetyo. 2006. *"Bisnis E-Commerce Studi Sistem Keamanan dan Hukum di Indonesia"*. Yogykarta : Pustaka Pelajar

Afandi Irfan Arif, Ari Kusyanti, Niken Hendrakusuma Wardani. *"Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, dan Perilaku Keamanan Pada Para Pengguna Media Sosial Line".* Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya

Batmetan John Reimon,, Morisa F.Lumingkewas, Claudia Tumuyu, Putri P.Ante *"Analisis Perilaku Kemanan Informasi Pengguna Sosmed Dikalangan Generasi Milenial"*. Prodi Pendidikan Teknologi Informasi dan Komunikasi, Universitas Negeri Manado, Tondano. 95318

M. L. Tompodung, F.Supit, J. R. Batmetan,*"Rancang Bangun Aplikasi Sensus Penduduk Berbasis Android"*, Buletin Saruputra, 2017, vol.7, pp. 57-61

Paramitha, Cindy Rizal Putri, 2011. *"Analisis Faktor Pengaruh Promosi Berbasis. Sosial Media Terhadap Keputusan Pembelian Pelanggan dalam Bidang.*"

Priyantdoyo, A. (2006). *"Vulnerability Assesment untuk Meningkatkan Kesadaran Pentingnya Kemanan Informasi"*. Jurnal Sistem Informasi

Putra Ariep Pratama, Dedy Syamsuar,S.KOM.,M.I.T, Andri,M.CS. "*Implementasi Penetrasi Testing Untuk Mengetahui Keamanan Penggunaan Aplikasi Sosial Media Menggunakan Metode Action Reserch".* Dosen Universitas Bina Darma, Mahasiswa Universitas Bina Darma Jalan Jenderal Ahmad Yani No.12 Palembang.