Analisis Teknik Penyerangan *Phishing* Pada *Social Engineering* Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi *Black Eye* dan *Setoolkit*

Sri Wahyuni¹, Irfan Murti Raazi² dan Ima Dwitawati³

Program Studi Teknologi Informasi, Fakultas Sains & Teknologi,

Universitas Islam Negeri Ar-Raniry, Banda Aceh

Email : Sri.wahyuni@ar-raniry.ac.id¹, irfanmurtiraazi@gmail.com², ima@ar-raniry.ac.id³

Abstrak - Di era teknologi yang kian maju dan berkembang luas seperti sekarang ini, informasi merupakan aset yang sangat perlu dilindungi oleh suatu organisasi ataupun individu, informasi yang bersifat privasi penting untuk dilindungi agar tidak dapat diakses oleh pihak yang tidak berwenang. Penyerangan *social engineering* hingga saat ini masih terus meningkat, hal ini terjadi karena pelaku mengetahui bahwa rantai terlemah pada sistem keamanan jaringan itu sendiri ialah pengguna, sehingga perancangan sistem keamanan yang baik harus disertai pemahaman tentang penyerangan dan ancaman oleh pengguna itu sendiri. Adapun tujuan penulisan artikel ini untuk dapat menjelaskan teknik penyerangan dengan memanfaatkan manipulasi psikologis yang dilakukan berdasarkan bagaimana cara korban berpikir dan bertindak. Teknik penyerangan *phishing email spoofing* adalah salah satu jenis penyerangan *social engineering* yang dilakukan dengan menggabungkan *black eye* dan *setoolkit*. Sehingga dapat memberikan informasi terkait dalam mengambil tindakan dalam melakukan suatu hal tentang *social engineering* dan acamannya.

Kata kunci : *Social engginering, Phishing, Email Spoofing, Black Eye, Setoolkit*

Abstract - In the era of increasingly advanced and widespread technology as it is today, information is an asset that really needs to be protected by an organization or individual, information that is privacy is important to protect so that it cannot be accessed by unauthorized parties. Social engineering attacks are still increasing, this happens because the hacker know that the weakest chain in the network security system itself is the user, so that a good security system design must be accompanied by an understanding of attacks and threats by the users themselves. The purpose of writing this article is to be able to explain attack techniques by utilizing psychological manipulation that is carried out based on how the victim thinks and acts. Email spoofing phishing attack technique is one type of social engineering attack that is carried out by combining black eye and setoolkit. So that it can provide information related to taking action in doing something about social engineering and its threats.

Keywords : *Social engginering, Phishing, Email Spoofing, Black Eye, Setoolkit*

1. Pendahuluan

Di era teknologi yang kian maju dan berkembang luas seperti sekarang ini, kemampuan dan rasa keingintahuan manusia dalam menguasai teknologi juga semakin meningkat. Hal ini sejalan dengan kemunculan beragam jenis kejahatan dunia maya. *Cybercrime* (kejahatan dunia maya) merupakan istilah yang dipakai untuk tindak kejahatan yang menggunakan jaringan komputer dengan penyalahgunaan teknologi digital sebagai alat kejahatan. *Cybercrime* ini tidak jauh dari permasalahan sistem keamanan jaringan, bila dikaitkan dengan informasi sebagai aset dalam menerapkan kehandalan dalam penerapan keamanan jaringan [1]. Namun, tidak semua *cybercrime* murni dilakukan dibalik layar atau hanya fokus mengeksploitasi mesin, akan tetapi juga menyerang langsung pada pengguna komputer. Biasanya teknik ini digunakan untuk penyebaran *malware* atau untuk mendapatkan informasi yang diperlukan oleh peretas, seperti identitas seseorang.

Social engineering adalah penyerangan dengan teknik memanipulasi dan memanfaatkan kesalahan manusia untuk mendapatkan suatu informasi. Adapun bentuk serangan yang dilakukan seperti penipuan dan pencurian data. Penipuan yang didasarkan pada manipulasi psikologis dilakukan dengan menganalisis cara korban berpikir dan bertindak sehingga dapat mengelabui dan memengaruhi korban. Hal ini sangat sering terjadi disekitar kita dimana target penyerangan tidak menyadari dan melayani instruksi penyerang. *Social engineering* ini terjadi karena *hacker* (penyerang) mengetahui bahwa semua pengguna dapat menjadi rantai terlemah pada suatu sistem keamanan jaringan. Oleh sebab itu, selain minimnya pengetahuan pengguna terkait mekanisme perangkat keamanan, seperti *social engineering* juga menjadi salah satu alasan sistem mudah diserang oleh *hacker* [2].

Phishing merupakan salah satu bentuk kegiatan kriminal dengan menerapkan *social engineering*. Diantara salah satu bentuk kegiatan dari teknik *phishing* ialah *email spoofing*. *Email spoofing* adalah teknik yang sering digunakan oleh *spammer* ke jutaan pengguna email dengan memanipulasi target seolah-olah berasal dari institusi resmi yang dapat mengarahkan target untuk melakukan kegiatan *phishing* [3]. Hal ini menyebabkan banyaknya terjadi kasus kebocoran informasi rahasia yang dikirimkan melalui email serta tindakan pemalsuan pesan atau identitas dengan tujuan untuk melakukan pencurian data pribadi. Penyerangan melalui email juga didasari tingginya penggunaan email karena selain sebagai media untuk mengirim dan menerima pesan, email juga dimanfaatkan sebagai media untuk memvalidasi informasi rahasia yang terhubung dengan berbagai akun media sosial[4]. Pada artikel ini akan melakukan analisis terhadap penyerangan yang dilakukan melalui email dengan teknik web phishing menerapkan email spoofing. Adapun aplikasi yang digunakan adalah kombinasi black eye dan setoolkit. Hasil percobaan akan menjadi rujukan terhadap kerentanan penyerangan dalam bentuk social engineering sehingga dapat meningkatkan kewaspadaan dan penentuan tindakan preventif pada setiap pengguna.

2. Tinjauan Pustaka

2.1 Social Engineering

Social engineering adalah suatu tindakan yang memanipulasi seseorang menggunakan salah satu cara dengan tindakan tertentu atau mencari kelemahan target agar dapat memperoleh informasi, akses, serta dapat mendorong target untuk dapat melakukan aksinya [2]. Terdapat beberapa pola dalam *social engineering* yang dilakukan oleh para *hacker*, diantaranya adalah sebagai berikut:

1. Mengumpulkan informasi, informasi yang didapatkan berupa struktur suatu organisasi, nama, dan sebagainya dalam perkembangan relasi dengan targetnya.
2. Relasi, usaha dalam melakukan interaksi dengan salah satu target agar dapat memperoleh informasi dari target, dengan syarat target mempercayai pelaku.
3. Mengeksploitasi, adanya usaha dalam mengeksploitasi informasi yang telah didapatkan dari pihak yang terlibat untuk masuk ke suatu sistem.
4. Eksekusi, *hacker* akan melakukan penyerangan sistem dengan mudah seperti mencuri, merubah dan bahkan dapat merusak sistem keamanan [5].

Dalam hal ini komponen terlemah dari sistem keamanan ialah manusia, karena penyerang akan melakukan berbagai cara agar dapat memperoleh informasi rahasia dari teknik manipulasi terhadap seorang hingga dapat memberikan akses masuk ke dalam sistem[6]. Adapun teknik *Social engineering* terbagi menjadi dua jenis sebagai berikut :

1. Berbasis Interaksi sosial, yaitu penyerang akan melakukan komunikasi dengan korban sehingga dapat memperoleh informasi. Bentuk interaksi yang sering dilakukan adalah:
 - a. *Shoulder surfing*, dilakukan dengan cara mengamati tingkah laku korban dengan sasaran untuk mendapatkan informasi tertentu.
 - b. *Hoaxing*, penyebaran informasi yang tidak sesuai dengan fakta sehingga dapat membuat target akan percaya dari informasi yang diberikan.
 - c. *Creating confusion*, pelaku akan membuat target kebingungan dalam hal tertentu dan kemudian memanfaatkan kesempatan tersebut.
 - d. *Impersonation*, pelaku akan meniru identitas atau melakukan penyamaran agar dapat akses legal ke sistem komputer.
 - e. *Reverse social engineering*, teknik yang memanipulasi dengan cara menawarkan bantuan kepada korban untuk mendapatkan keuntungan bagi pelaku dari tawaran yang diberikan [2].
2. Berbasis interaksi komputer, yaitu penyerang akan menggunakan komputer dalam mendapatkan informasi. Bentuk interaksi komputer yang dapat dilakukan adalah sebagai berikut :
 - a. *Phishing*, penyerangan dengan teknik memanipulasi psikologis target untuk mendapatkan informasi penting. Penyerangan ini dalam bentuk penipuan dengan menyebar pesan-pesan palsu yang didalamnya disisipkan URL berbahaya.
 - b. *Brand spoofing*, adalah bentuk pemalsuan terhadap suatu *brand* atau merek tertentu.
 - c. *Baiting*, adalah bentuk serangan yang dilakukan dengan memberikan iming-iming hadiah dan sejenisnya sama halnya seperti *phishing*. Bahkan *baiting* dapat membuat sebuah iklan *software* untuk menarik target hingga mengunduh aplikasi yang berisikan malware [1].

2.2 Email (Electronic Mail)

Email adalah suatu alat komunikasi berupa surat elektronik yang diterapkan pada perangkat seperti komputer. Layanan email dapat digunakan pada saat terhubung dengan internet. Alamat email ini gabungan dari nama pengguna dan *domain name*. layaknya surat konvensional, alamat email menjadi salah satu identitas

yang menunjukkan alamat unit seseorang. Pesan email dapat terdiri dari berbagai layanan media, baik berupa teks, gambar maupun video dengan berbagai format lampiran [7]. *Elektronik mail* (E-mail) merupakan sebuah media komunikasi antara satu pihak dengan pihak lainnya yang kini sangat populer. Dalam mengirim dan menerima email, dibutuhkan sebuah layanan (*server*) pada email. *Mail Server* adalah sebuah program yang dapat menyebarkan *file* atau informasi sebagai tindakan dalam merespon permintaan yang dikirim lewat email untuk saling berkomunikasi satu dengan yang lainnya melalui sebuah jaringan internet [8].

Dalam hal ini salah satu teknik *phishing* yang digunakan oleh *hacker* adalah email *spoofing*. Email *spoofing* digunakan oleh *hacker* dengan cara mengirimkan email secara *broadcast* ke semua pengguna, selayaknya dari salah satu organisasi resmi yang melakukan komunikasi [3]. Dimana penyalahgunaan dalam menggunakan email yang sering terjadi bertujuan untuk mencuri informasi agar mendapatkan hak akses tidak sah. Berikut ini beberapa penerapan penyalahgunaan pada email :

- Spam*, adanya pesan masuk yang tidak diinginkan, biasanya dikirim tidak hanya sekali yang mana hal ini juga menyebabkan meningkatnya konsumsi sumber daya.
- Penipuan (*Scam*), tindakan yang dilakukan oleh penyerang untuk menipu korban dalam suatu transaksi, tindakan yang dilakukan biasanya telah digabungkan dengan *phishing*.
- Penyebaran *URL Phishing*, adanya sebuah tautan palsu yang dapat menyerupai situs aslinya.
- Email spoofing*, sebuah teknik yang dipakai oleh *spammer* dan *scammer* dalam menyamar sebagai salah satu unit organisasi untuk menyembunyikan asal usul pesan email. Pengirim *email spoofing* akan membuat sebuah email yang akan sesuai dengan pengirim aslinya [9].

2.3 Media Sosial

Media sosial adalah sebuah *platform* yang dapat mewujudkan interaksi sosial di era perkembangan teknologi informasi yang bersifat interaktif dengan berbasis teknologi internet. Sifat interaktif dapat menciptakan berbagai pola penyebaran informasi dari satu pihak ke pihak lainnya. Sehingga dengan kehadiran media sosial akan berpotensi merubah pola interaksi sosial, baik dalam tingkat individu ataupun komunitas. Namun, media sosial tidak hanya digunakan dalam konteks pribadi dalam mencari kepopuleran, akan tetapi juga digunakan dalam kepentingan profesional, salah satunya LinkedIN [10].

LinkedIN merupakan suatu media sosial profesional dengan 443 juta pengguna dari 200 negara. Oleh karena itu, LinkedIN menjadi salah satu platform untuk rekrutmen para pencari kerja dan perusahaan yang membutuhkan tenaga kerja. Hal ini sangat menguntungkan kedua belah pihak dimana perusahaan yang membutuhkan tenaga kerja telah membangun hubungan dengan client jauh sebelum mereka melamar ke perusahaan [11].

3. Metode Penelitian

Metode yang dipakai dalam penelitian ini adalah studi kepustakaan atau literatur, yaitu studi objek penelitiannya berbentuk karya-karya kepustakaan, baik berupa jurnal ilmiah buku, serta data-data statistik. Kepustakaan tersebut akan dipakai untuk menjawab permasalahan penelitian yang diajukan penulis untuk menggambarkan bagaimana bentuk serangan *phishing email spoofing* dapat dilakukan dengan mudah. Pada penelitian ini percobaan dilakukan dengan menggunakan aplikasi *black eye* dan *setoolkit* dalam mengambil kredensial milik pengguna.

Dalam hal ini penelitian yang digunakan adalah studi kasus dengan fokus penelitian adalah penyalahgunaan email dalam melakukan *spamming* email pada media sosial profesional LinkedIN yang telah disisipkan URL berbahaya. Dengan demikian, *phishing* yang dilakukan berupa *cloning* suatu situs website menggunakan *black eye*, dimana *black eye* akan menghasilkan alamat URL palsu namun terlihat seperti URL asli karena bersifat SSL atau ditandai dengan protokol HTTPS (*Hypertext Transfer Protocol Secure*). Adapun *Tools* dan aplikasi yang digunakan dalam penelitian ini adalah sebagai berikut:

- Black Eye dan Social Engineering Toolkit (Setoolkit) yang sudah terinstal pada sistem operasi Kali Linux
- Media sosial profesional LinkedIN
- Email Target

4. Hasil Dan Pembahasan

4.1 Tahapan Black Eye

Dalam *tool Black Eye* terdapat berbagai macam *template* yang tersedia untuk halaman *phishing*, *template* yang tersedia pada *black eye* Sebagian besar berasal dari situs web populer yang banyak digunakan oleh pengguna milenial juga tersedia opsi untuk *template phishing* khusus (*Custom*). Dengan desain *template* yang telah dipilih selanjutnya *Black Eye* akan melakukan *cloning* website. Laman website hasil dari *cloning* dapat disebarkan ke target dengan berbagai cara, seperti email, pesan ataupun melalui media sosial lainnya

Gambar 1. Tahap Persiapan *Black Eye*

4.2 Tahapan Setoolkit

Setoolkit bagian dari pentest berbasis Python *open-source* yang ditujukan untuk social engineering, yang mana pada Setoolkit menyediakan beragam fitur yang dapat digunakan dalam *social engineering*, diantaranya *cloning* website, phishing, dan lain sebagainya. Pada menu email mass mailer yang digunakan dapat melakukan *spamming* berupa pesan yang sama ke daftar email target dengan menerapkan teknik email *spoofing*. Dimana pesan yang dikirimkan telah dilengkapi dengan URL phishing dari tahapan *black eye* terdahulu.

Gambar 2. Tahap Persiapan Setoolkit

4.3 Hasil Percobaan

1. Proses *Cloning* Website LinkedIn Menggunakan *Tool Black Eye*

Pada tool *Black Eye* dipilih *template* no.9 *LinkedIN* untuk selajutnya membuat *cloning* website dengan menggunakan URL oleh protocol *HTTPS*. Tampilan seperti pada gambar dibawah ini.

Gambar 3. *Cloning* Website LinkedIN

2. Proses *Phishing* Email *Spoofing* Menggunakan Setoolkit

Persiapan pengiriman email dimulai dari penentuan subject yang tepat dan deskripsi pesan yang meyakinkan. Hal ini dilakukan untuk memastikan email terlihat cukup berkesan sehingga menarik perhatian target penerima. Pengiriman pesan dilakukan kepada seluruh penerima yang telah terdaftar, masing-masing

file akan terbaca secara baris perbaris. Adapun notifikasi pengiriman email berhasil akan dapat terlihat dari setoolkit.

```
setoolkit> Your gmail email address:irfanmurtiraazi@gmail.com
setoolkit> The FROM NAME the user will see:LinkedIn
Email password:
setoolkit> Flag this message's as high priority? (yes/no):no
Do you want to attach a file - (y/n): n
Do you want to attach an inline file - (y/n): n
setoolkit> Email subject:Important LinkedIn Message
setoolkit> Send the message as html or plain? 'h' or 'p' (p):p
setoolkit> When finished, type CMD (All capital) then hit (return) on a new line.
setoolkit> Enter the body of the message, type CMD (capital) when finishedHello, how are you? You received a message from LinkedIn. It's been marked as urgent, che
ck it now : https://f4d7-182-3-5-90.ngrok.io
Next line of the body:
Next line of the body: END
```

Gambar 4. Proses *Phishing* Email

Gambar 5. Hasil Pengiriman Email Dari Setoolkit

Gambar 6. Hasil Isi Pesan Target

Berikut ini adalah hasil isi pesan dari salah satu target yang mendapatkan notifikasi gmail dan melanjutkan instruksi pada akan laman URL *phishing*. Dimana target telah berada di halaman website *phishing cloning* www.linkedin.com yang menghasilkan halaman web utama yang layaknya LinkedIn yang sebenarnya.

Selanjutnya target melakukan *login* ke halaman tersebut. Informasi akun dan kata sandi telah berhasil diperoleh pada terminal pelaku.

Gambar 7. Halaman *Phishing Cloning* LinkedIn

Gambar 8. Hasil Kredensial

5. Kesimpulan

Berdasarkan dari hasil pembahasan yang dilakukan menunjukkan bahwa *Social Engineering* merupakan salah satu teknik penyerangan yang dapat dengan mudah dilakukan. Hal tersebut didasari oleh pemanfaatan kelemahan sisi psikologis pengguna untuk dapat menjadi celah terjadinya pencurian informasi. teknik manipulasi yang dapat dilakukan dapat berupa Phishing dengan email spoofing menggunakan kombinasi black eye dan setoolkit. Dengan demikian, berdasarkan hasil penelitian ini diharapkan dapat memberikan pengetahuan tentang salah satu penyerangan *Social Engineering* menggunakan teknik *phishing* dengan *email spoofing* sebuah website yang sangat umum digunakan. Selain itu agar dapat waspada terhadap berbagai metode *Social Engineering* lainnya dengan lebih memperhatikan setiap pesan yang diterima, menaruh curiga pada kejanggalan dari isi pesan, serta melakukan konfirmasi ulang pada pihak terkait bilamana terdapat hal-hal yang menjadi perhatian.

Daftar Pustaka

- [1] I. R. Hidayah, "Representasi Social Engineering Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall)," *Tibannndaru J. Ilmu Perpust. dan Inf.*, vol. 4, no. 1, p. 30, 2020.
- [2] E. M. Safitri, Z. Ameilindra, and R. Yulianti, "Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur," *J. Ilm. Teknol. ...*, vol. 2, pp. 21–26, 2020.
- [3] Z. Efendy, I. E. Putra, and R. Saputra, "Asset Rental Information System and Web-Based Facilities At Andalas University," *J. Terap. Teknol. Inf.*, vol. 2, no. 2, pp. 135–146, 2019.
- [4] L. Silalahi and A. Sindar, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, 2020.
- [5] D. I. Junaedi, "Antisipasi Dampak Social Engineering Pada Bisnis Perbankan," *Infoman's*, vol. 11, no. 1, pp. 1–10, 2017.
- [6] Y. Yanti, M. Munawir, Z. Zulfan, and E. Erdiwansyah, "Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain," *J. Serambi Eng.*, vol. 2, no. 4, 2017.
- [7] M. S. Rumetna, "KOMBINASI GNU PRIVACY GUARD DAN HAMMING DISTANCE UNTUK KEAMANAN EMAIL SERTA JALUR SERTIFIKASI COMBINATION OF GNU PRIVACY GUARD AND HAMMING DISTANCE FOR EMAIL SECURITY AND CERTIFICATION PATHS," *J. Elektro Luceat*, vol. 7, no. 2, 2021.
- [8] A. Faruq, K. Khaeruddin, and M. Lestandy, "Sistem Keamanan Multi Mail Server Dengan Teknik Enkripsi Openpgp Pada Zimbra Exchange Open Source Software," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 3, pp. 493–500, 2020.
- [9] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016.

- [10] A. Sapotri and T. Pannindriya, "MEDIA SOSIAL INSTAGRAM Stretched Social Interaction by Nowadays Doctor Through Instagram as Social Media," *J. Magister Ilmu Komun.*, vol. 5, no. 2, pp. 121–140, 2019.
- [11] H. Muhammad, M. Putra, M. H. Fahamsyah, P. S. Manajemen, and U. P. Bangsa, "PENERAPAN PLATFORM MEDIA SOSIAL LINKEDIN SEBAGAI ALAT," *J. Investasi*, vol. 7, no. 4, pp. 15–24, 2021.