Analisis Serangan Keamanan Informasi Pribadi Pada Media Sosial Facebook Menggunakan Metode *National Institute of Justice* (NIJ)

Khairani Rahmatul Ummah[1)], Dahliyusmanto[2)]

[1)]Mahasiswa Jurusan Teknik Informatika, [2)]Dosen Jurusan Teknik Informatika Fakultas Teknik Universitas Riau
Kampus Binawidya Jl. HR. Soebrantas Km 12,5 Pekanbaru 28293
khairani.rahmatul@student.unri.ac.id

ABSTRACT

Social media is very important in everyday life. However, when used, a lot of personal data and information is shared. This risks being vulnerable to personal data leaks. Facebook is one of the social media that often experiences user data leaks. There are many ways to steal Facebook user data, one of which is by using Phishing techniques. Phishing means tricking a user into entering a username, password, or other personal data on a modified site. This research was conducted regarding Phishing attacks. The method used is the National Institute of Justice (NIJ). The stages flow starts from the preparation stage, the collection stage, the examination stage, the analysis stage, and the reporting stage. The Wireshark application was used to search for evidence, and the Hashcalc application was used to acquire the obtained evidence.

Keywords: *Facebook, phishing, cybercrime, Wireshark.*

1. PENDAHULUAN

Jejaring sosial menjembatani komunikasi, baik komunikasi dengan teman lama atau mencari teman baru. Di era perkembangan teknologi yang pesat, internet telah menjadi segalanya dalam aspek kehidupan. Facebook adalah salah satu media sosial yang paling populer. Dalam penggunaannya, Facebook mengumpulkan banyak data pengguna, dimulai dari nama, tanggal lahir, alamat email, dan data pribadi lainnya. Data pribadi yang diunggah ke internet, rentan mengalami kebocoran data dan menjadi objek kejahatan dunia maya (*cyber crime*).

Ada banyak kasus kejahatan dunia maya, salah satunya serangan Phishing. Serangan Phishing yakni pelaku membuat tiruan dari website yang mirip dengan website asli. Calon korban akan diminta memasukkan nama pengguna dan kata sandi ke situs yang sudah dimodifikasi. Pengguna yang tidak berhati-hati akan memasukkan datanya. Hal itulah yang dimanfaatkan oleh pelaku.

Oleh karena pada penelitian ini, peneliti akan melakukan skenario Phishing dengan tujuan menganalisis serangan Phising menggunakan metode *National Institute of Justice* (NIJ).

2. STUDI PUSTAKA

2.1. Penelitian Terkait

Penelitian yang dilakukan oleh Aseh Ginanjar pada tahun 2018 yang berjudul Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process. Penelitian ini menggunakan metode NFP dalam mengatasi Phishing.

Penelitian yang dilakukan oleh Muhammad Aziz, Imam Riadi, dan Rusydi Umar pada tahun 2018 yang berjudul Analisis Forensik Line Messenger Berbasis Web Menggunakan Framework *National Institute of Justice* (NIJ) yaitu, menjelaskan metode yang digunakan untuk penelitian ini menggunakan metode *National Institute of Justice* (NIJ).

2.2. Facebook

Facebook adalah layanan jejaring sosial yang didirikan oleh Mark Zuckerberg sejak tahun 2004. Facebook dengan cepat menjadi salah satu media sosial populer yang mengumpulkan 2,8 juta pengguna di seluruh dunia terhitung sampai Juni 2021.

Sejak dikembangkan pada tahun 2004, Facebook sudah menjadi sasaran tindak kejahatan yang mengintai data pribadi penggunanya. Beberapa kasus pencurian data Facebook di antaranya menyerang secara

pribadi ataupun secara berkelompok.

Kasus pembobolan secara berkelompok umumnya menjaring banyak korban dengan link palsu yang dibagikan di Facebook. Link itu berisi halaman website yang meminta pengguna untuk mengisi data pribadi seperti nama pengguna dan kata sandi. Jika pengguna tidak hati-hati, maka data mereka akan mudah didapatkan oleh pelaku.

2.3 Serangan Kejahatan Dunia Maya

Serangan kejahatan dunia maya (*cybercrime*) merupakan aktivitas seseorang, sekelompok orang, atau badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan dan komputer sebagai sasaran (Widodo, 2013). Selanjutnya, Organization of European Community Development (OECD) mengeluarkan definisi lebih lanjut tentang kejahatan dunia maya sebagai "*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*" yang memiliki artian setiap tindakan ilegal, tidak etis, atau tidak sah terkait dengan pemrosesan otomatis dan/atau transmisi data. Menurut definisi ini, kejahatan komputer ini mencakup akses ilegal ke transmisi data. Oleh karena itu, dapat dilihat bahwa setiap aktivitas yang tidak sah dalam sistem komputer adalah kejahatan.

Phishing adalah salah satu penipuan online yang paling umum. Phishing datang dalam berbagai bentuk. Jenis penipuan ini biasanya meniru situs web yang kredibel seperti situs web bank atau akun media sosial yang seringkali berbeda dengan aslinya. Ada sedikit perubahan nama link jadi calon korban tidak menyadarinya. Seringkali, peretas mengirim email yang meminta calon korban untuk masuk ke akun bank-nya atau halaman akun lainnya untuk melakukan verifikasi informasi pribadi calon korban. Peretas mengirim tautan ke alamat halaman palsu. Namun, harap dicatat bahwa situs web resmi di atas tidak pernah meminta calon korban untuk melakukan hal itu.

2.4 Wireshark

Wireshark adalah salah satu dari sekian banyak perangkat lunak berbasis open source yang digunakan untuk menangkap lalu lintas jaringan dan menganalisis paket data dengan sangat detail (Widodo, 2012). Terkadang Wireshark juga disebut sebagai penganalisis jaringan atau sniffer. Semua jenis paket data dalam berbagai format log dapat dengan mudah direkam dan dianalisis.

3. METODOLOGI

Pada Penelitian ini menggunakan metode *National Institute of Justice* (NIJ). Metode ini membagi menjadi lima langkah yakni *identification*, *collection*, *examination*, *analysis*, dan *reporting.*

3.1 Hardware dan Software yang Digunakan

Penelitian ini dilakukan dengan menggunakan perangkat keras (*hardware*), perangkat lunak (*software*), dan situs-situs yang menganalisa Phishing. Penelitian ini dilakukan menggunakan 1 laptop, milik investigator dan 1 ponsel milik korban.

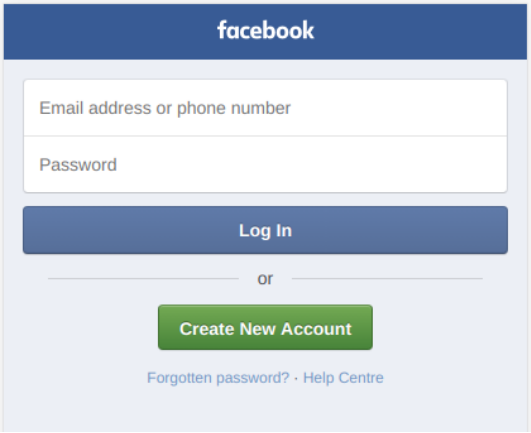
Hardware	Software	Website
Prosesor Intel(R) Pentium(R) CPU B940 @ 2.00GHz	Sistem Operasi Microsoft Windows 7, 32-bit	https://centralops.net
Graphics Intel® HD Graphics	Wireshark-win32-3.6.0	
RAM 2.00GB	Hashcalc	
Harddisk 361GB	Google Chrome Version 96.0.4664.110 (32-bit)	

3.2 Simulasi Kasus Kejahatan

Skenario kasus kejahatan dimulai ketika pengguna mendapat pemberitahuan (notifikasi) yang meminta pengguna untuk melakukan konfirmasi data diri pada Facebook.

Gambar 1. Masuk Pemberitahuan Login

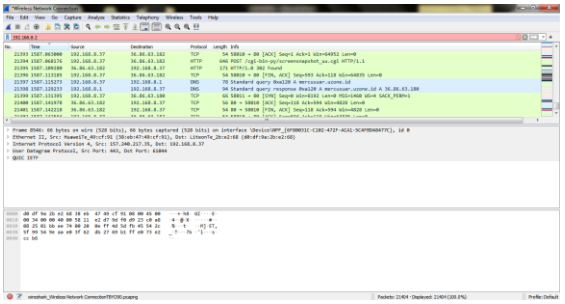
Gambar 1 menunjukkan bahwa pengguna harus mengkonfirmasi data dirinya dengan menekan tautan yang diberikan. Di waktu yang sama, investigator melakukan *capture* pada Wireshark ketika pengguna menekan tautan. Hal itu dilakukan untuk mendapat barang bukti dan segera dikumpulkan agar tidak ada perubahan data dari barang bukti tersebut.



Gambar 2. Pengguna Login

4. Pembahasan dan Hasil

Penelitian ini mengikuti tahapan *National Institute of Justice* (NIJ) yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*. Pada tahap identifikasi, investigator mengidentifikasi bahwa ada link yang diduga link Phishing. Investigator kemudian mengumpulkan data (*collection*) dengan melakukan *capture* jaringan menggunakan Wireshark.



Gambar 3. Hasil Capture

Barang bukti berupa *capture* kemudian diperiksa (*examination*) menggunakan aplikasi Hashcalc, dipergunakan untuk memperoleh informasi *file hash* dari hasil *capture*. Setelah itu dilakukan analisis dari barang bukti dari hasil *capture* dan nilai *hash.*

Pada tahap analisis, paket data akan difilter untuk memudahkan mencari paket yang dibutuhkan. Kata kunci DNS yang berhubungan dengan link yaitu https://telegra.ph/NOTIFICATION-08-20 dengan IP server 149.154.164.13. Data ini dijadikan barang bukti yang berhubungan dengan domain tersebut.

Setelah diketahui DNS dari link Phishing tersebut, investigator melakukan mengecekan melalui situs centraloops.net

Gambar 4. Informasi Penyerang

Gambar 4 menunjukkan informasi penyebar link Phishing. Diperoleh informasi sebagai berikut:

Nama Domain : telegra.ph
Pembuat Domain : Nikolai Durov
Tanggal Domain : 19 September 2014
Lokasi Domain : British Virgin Islands

Tahap terakhir adalah melaporkan (*reporting*) hasil analisis barang bukti dari hasil *capture* jaringan dan pencarian DNS penyerang.

5. Kesimpulan

Dengan mengikuti tahapan *National Institute of Justice* (NIJ) dapat dilakukan *reporting* mengenai serangan Phishing. Investigator berhasil menemukan barang bukti, IP address, dan lokasi pembuat domain link Phishing.

DAFTAR PUSTAKA

Widodo. (2013). Aspek Hukum Pidana Kejahatan Mayantara. Yogyakarta: Aswaja Pressindo.

Widodo, S. (2012). Pemantauan Jaringan Komputer dengan DNS Server Berbasis Routing Statis Menggunakan Wireshark. Jurnal Teknik Elektro, 1(2), 1–7