JURNAL TEKNIK MESIN, ELEKTRO DAN ILMU KOMPUTER

Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/teknik
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

ANALISIS KERENTANAN KEJAHATAN ONLINE PHISING MENGGUNAKAN TOOLS ZPHISHER, SHELLPHISH DAN WHPHISHER

Ni Komang Arista Tri Wahyuni [a], Putu Putri Cahayani [b], I Gusti Ngurah Yogi Wicaksana [c], Ida Ayu Kadek Bintang Wijayanti[d]

[a] Fakultas Teknik dan Kejuruan/ Teknik Informatika, arista.tri @undiksha.ac.id, Universitas Pendidikan Ganesha
[b] Fakultas Teknik dan Kejuruan/ Teknik Informatika, putri.cahayani @undiksha.ac.id, Universitas Pendidikan Ganesha
[c] Fakultas Teknik dan Kejuruan/ Teknik Informatika, yogi.wicaksana @undiksha.ac.id, Universitas Pendidikan Ganesha
[d] Fakultas Teknik dan Kejuruan/ Teknik Informatika, ayu.bintang.wijayanti@undiksha.ac.id, Universitas Pendidikan Ganesha

ABSTRAK

In the era of increasingly advanced and widespread technology as it is today, personal data is an asset that really needs to be protected by an organization or individual, personal data information that is private is very important to be protected so that it cannot be accessed by unauthorized parties. Phishing attacks are currently still increasing, this happens because the perpetrators of phishing attacks understand to trick victims where the victim is still weak to understand the security system on personal data information. The purpose of this article is to explain how these phishing attacks can still be carried out, so that technology users can better understand phishing attacks and further improve the security of users' personal data themselves. Website phishing attack technique is one type of phishing attack that can be done with several types of tools including Zphisher, Shellphish and WhPhisher. With the exposure of this article, technology users get information regarding phishing website attacks and actions to deal with them.

Keywords: website phishing, Zphisher, Shellphish, WhPhisher

Abstrak

Di era teknologi yang semakin maju dan meluas seperti sekarang ini, data pribadi merupakan aset yang sangat perlu dilindungi oleh suatu organisasi maupun individu, informasi data pribadi yang bersifat privasi sangat penting untuk dilindungi, tujuannya agar tidak dapat diakses oleh pihak yang tidak berkepentingan. Serangan pengelabuan/ phishing saat ini masih meningkat, hal ini terjadi karena pelaku serangan phising mengerti untuk mengelabuhi korban yang dimana korban tersebut masih lemah untuk memahami sistem keamanan pada informasi data pribadi. Tujuan dibuatnya artikel ini ialah untuk menjelaskan bagaimana serangan phishing ini masih dapat dilakukan, sehingga pengguna teknologi dapat lebih memahami serangan phishing dan lebih meningkatkan keamanan data pribadi pengguna itu sendiri. Teknik penyerangan phishing website adalah salah satu jenis serangan phishing yang dapat dilakukan dengan beberapa jenis tools diantaranya zphisher, shellphish dan whphisher. Dengan pemaparan artikel ini, pengguna teknologi mendapatkan informasi terkait serangan website phishing dan tindakan dalam menangani hal tersebut.

Kata kunci: website phishing, Zphisher, Shellphish, WhPhisher

1. PENDAHULUAN

Seiring berkembangnya zaman maka berkembangnya pula suatu kemajuan yang ada di dunia [1]. Baik dari segi pengetahuan, ekonomi, budaya, termasuk teknologi dan lain-lain [1]. Pesatnya perkembangan yang telah dilalui selama ini juga memberikan dampak yang baik bagi manusia namun tidak dapat dipungkiri juga terdapat dampak buruknya [1]. Teknologi menjadi perkembangan yang dikatakan pesat dari masa ke masa [2]. Pesatnya perkembangan teknologi juga membuat manusia memiliki banyak inovasi untuk kemajuan teknologi [2]. Meski banyak inovasi teknologi yang telah berkembang, tidak dapat dipungkiri bahwa zaman serba teknologi juga memiliki kejahatan [3]. Kejahatan sekarang tidak hanya secara kehidupan nyata saja namun telah merambat ke

Received February 27, 2023; Revised March 17, 2023; Accepted March 24, 2023

dunia maya yang dapat kita sebut dengan tindak kejahatan *online* [3]. Saat ini banyak sekali tindak kejahatan *online* yang terjadi di dalam aktivitas dunia maya [3]. Hal ini dapat menimbulkan keresahan pengguna *online* [3]. Jika menjadi korbannya, maka kita banyak mendapatkan kerugian [3].

Dari banyaknya jenis tindak kejahatan *online*, salah satunya yaitu *Phishing* [3]. Disini kita akan mencari hal mengenai *phishing*. Laporan ini dibuat dengan tujuan mendapatkan pengetahuan dan tidak untuk tindak kejahatan. *Phishing* yang dibahas adalah *facebook phishing*, dimana ini merupakan suatu tindak kejahatan *online* ketika seseorang mencoba mendapatkan akses ke akun *facebook* pengguna.

2. TINJAUAN PUSTAKA

2.1. Phising

Phising merupakan kejahatan digital yang menargetkan informasi atau data sensitif korban melalui email, unggahan media sosial, atau pesan teks. Dengan kata lain, phising, merupakan sebuah serangan yang dilakukan untuk menipu atau memancing korban agar mau mengklik link atau tautan serta menginput informasi kredential seperti username dan password. Pelaku phising biasanya menampakkan diri sebagai pihak atau institusi yang berwenang. Mereka menyisipkan tautan didalam narasi yang disebarkan dan menggiring korban agar mengklik tautan tersebut. Data yang menjadi sasaran phising adalah data pribadi seperti nama, usia, alamat dan data akun seperti username dan password, serta data finansial seperti informasi kartu kredit atau rekening bank. Informasi data yang diperoleh dari aktivitas phising nantinya akan dimanfaatkan untuk menipu orang bagi yang tidak bertanggungjawab. Data tersebut juga dapat dijual untuk melakukan tindakan yang tidak bertanggung jawab seperti penyalahgunaan akun. Menurut sebuah laporan, 32% pencurian data selalu melibatkan kegiatan phising. Bahkan, di awal tahun 2020 saja, Anti Phishing Working Group mencatat sudah ada 165.772 website phisingyang siap menjaring korban.

2.1.1. Cara Kerja Phising

Tahap awal kegiatan web phising akan dimulai dengan menentukan siapa calon korbannya. Pada umumnya, korban yang disukai adalah pengguna platform pembayaran online seperti Ovo, PayPal, dan lainnya. Tidak hanya itu saja, banyak pelaku phising yang mengincar pengguna platform yang memiliki celah keamanan. Kasus terbaru terjadi pada platform komunikasi Zoom**.** Tak kurang dari 1000 upaya phising terjadi hanya di bulan April 2020 saja**.** Setelah mendapatkan calon korban yang potensial, pelaku akan mulai memikirkan apa yang akan dicapai dari kegiatan web phising yang dilakukan. Apakah akan menarget username dan password pengguna untuk menguasai akun. Apa malah mendapatkan semua informasi korban melalui sebuah prosedur yang disiapkan. Pada contoh aksi phising PayPal, pelaku menginginkan semua informasi dari pengguna platform tersebut. Seperti ditunjukkan welivescurity.com, pengguna akan menerima email untuk mengkonfirmasi data diri melalui sebuah link website palsu yang disediakan.

Untuk melancarkan aksinya, pelaku akan mulai menyiapkan website palsu untuk melakukan aksi phising. Mulai dari mendesain website palsu, memilih nama domain yang mirip dengan domain asli hingga menyiapkan konten dengan tulisan yang meyakinkan. Pada prakteknya, pelaku kadang membuat website yang sangat menyerupai halaman website resmi tapi menggunakan nama domain yang jauh berbeda seperti terlihat di contoh atas.

Namun, pada contoh kasus phishing Danamon Online beberapa waktu lalu, Anda akan langsung melihat bahwa domain yang digunakan mirip sekali dengan website resminya. Dengan tampilan website dan informasi yang meyakinkan, tak sedikit calon korban yang akhirnya mengakses website phising milik pelaku. Langkah ini biasanya didahului dengan mengajak calon korban melalui email phising atau link yang disebarkan via SMS atau akun media sosial. Inilah kunci dari terjadinya aksi phising. JIka calon korban melakukan instruksi yang diberikan pelaku, maka pelaku akan berhasil mencapai tujuannya. Sebagai contoh, pada halaman website yang disediakan, calon korban diminta melakukan update informasi pribadi hingga data pembayaran pada akun yang digunakan. Pada saat selesai mengisi data dan melakukan submit, saat itulah semua informasi korban berhasil dimiliki. Jika aksi web phising berhasil, pelaku akan memanfaatkan data yang telah diterima.

3. METODOLOGI PENELITIAN

Website phising merupakan situs web yang dirancang untuk melakukan pengelabuan terhadap korban dengan cara percobaan untuk mendapatkan informasi sensitif, seperti nomor ip akun web, kata sandi aplikasi media sosial dan lainnya[1]. terdapat beberapa tahapan yang dilakukan *hacker* untuk mengelabuhi korban dengan cara melakukan *web phising*, *diantaranya* sebagai berikut:

1. Mencari dan melengkapi informasi, informasi-informasi yang dicari kemudian dikumpulkan oleh *hacker* sebagai tahap awal dilakukannya serangan *phising* ini tujuanya adalah untuk mendapatkan nama, nama akun korban[4].

2. Tahap kinerja, tahap ini bisa juga dikatakan dengan tahap Eksekusi, dimana pada tahap ini pelaku *hacker* akan melakukan serangan *phishing* dengan cara menggunakan tools *phishing* kemudian memberikan link kepada korban. sehingga *hacker* dapat mencuri data korban[5].

Tools yang dianalisis meliputi *ZPhisher*, *Shellphish* dan *WhPhisher*, akan ada analisis, pengukuran dan pengujian dalam metode penelitian ini.

a. Zphisher

- Analisis

Zphisher adalah *tools Phishing* berupa open-*source* yang kuat. *Tools* ini menjadi sangat populer saat ini yang digunakan untuk melakukan serangan phishing pada Target[3]. *Zphisher* lebih mudah daripada Toolkit Rekayasa Sosial[4]. *Tools* Ini berisikan beberapa *template* yang dihasilkan oleh tools yang disebut *Zphisher* dan menawarkan halaman web template phishing untuk 18 situs populer seperti *Facebook*, *Instagram*, *Google*, *Snapchat*, *GitHub*, *Yahoo*, *Protonmail*, *Spotify*, *Netflix*, *LinkedIn*, *WordPress*, *Origin*, *Steam*, *Microsoft*, dll[4]. *Tools* ini juga menyediakan opsi untuk menggunakan *template* khusus jika seseorang menginginkannya[4]. *Tools* ini memudahkan untuk melakukan serangan *phishing*[4]. Dengan menggunakan *tools* ini pengguna dapat melakukan serangan *phishing* di (jaringan area luas)[4]. *Tools* ini dapat digunakan untuk mendapatkan kredensial seperti id, kata sandi[4].

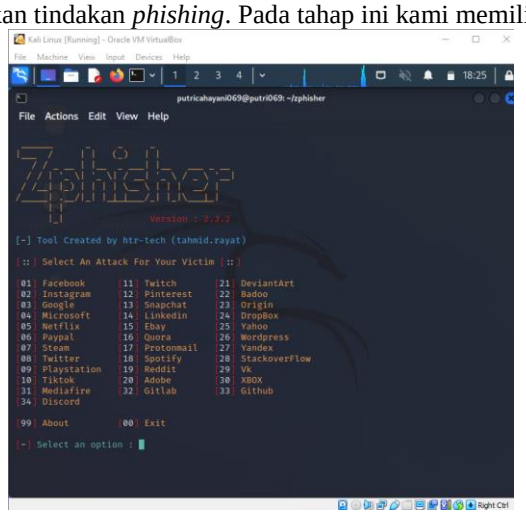
- Pengukuran

Pengukuran pada *tools phishing Zphisher* ini terdapat pada proses *phishing* yang dilakukan. *Tools* ini bekerja secara efektif saat digunakan pada percobaan phishing kami dikarenakan tools yang mudah dijalankan, respon tools yang cepat, terbukti dalam menjalankan tools ini memerlukan waktu 14,14 detik untuk menampilkan *link phishing* dan Memerlukan 6 tahapan untuk menampilkan *link phishing*, dimulai dari ***bash zphisher.sh*** untuk menampilkan pilihan situs web yang akan di akses.

- Pengujian

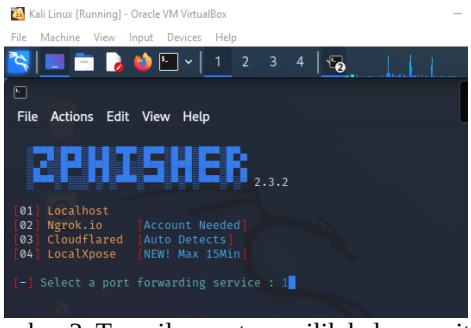
Pada pengujian pada tools *Zphisher* yang telah dikerjakan, terdapat beberapa tahapan dan hasil akhir dalam menjalankan *tools* ini, yaitu sebagai berikut.

1. Setelah menginstal *tools zphisher* di kali linux, tampilan selanjutnya adalah tampilan halaman situs populer untuk melakukan tindakan *phishing*. Pada tahap ini kami memilih aplikasi *facebook*.



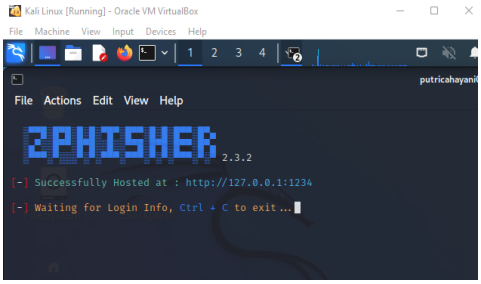
Gambar 1. Tampilan halaman situs

1. Setelah memilih opsi salah satu dari situs populer tersebut, tampilan selanjutnya adalah memilih opsi Localhost.



Gambar 2. Tampilan saat memilih halaman situs

2. Setelah meng input localhost kemudian pengguna akan mendapatkan link phishing yang nantinya akan diberikan kepada target.



Gambar 3. Tampilan saat link muncul

3. Setelah target membuka *link*, berikut merupakan tampilan *tools* berikutnya.

Gambar 4. Tampilan saat terget membuka link

b. Shellphish

- Analisis

ShellPhish adalah alat *phishing* yang ditulis dalam *bash* oleh *thelinuxchoice*[6]. *Shellphish* menawarkan total 18 situs web *phishing* dan satu situs web khusus yang dapat dikirim ke target[6]. Hal yang baik tentang alat ini adalah kita tidak perlu bersusah payah menyiapkan layanan hosting atau penerusan portal[6, hlm. 2].

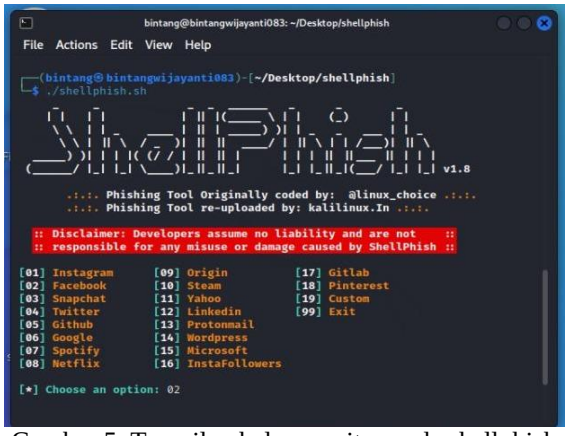
- Pengukuran

Pengukuran pada *tools phishing Shellphish* ini terdapat pada proses percobaan *phishing* yang telah dilakukan. *Tools* ini bekerja secara efektif pada saat penginstalan sampai dengan *phising* mengeluarkan *link* yang akan dikirimkan kepada target. Tetapi *tools* ini tidak bekerja secara efektif pada saat *link* tersebut dibuka. Untuk menjalankan *tools* ini memerlukan waktu sekitar 24,40 detik. Dan untuk mendapatkan *link* tahapan yang diperlukan sebanyak 3 kali klik dimulai dari ***chmod +x shellphish***, kemudian ***./shellphish.sh***, lalu pilih salah satu situs web yang akan diakses.

- Pengujian

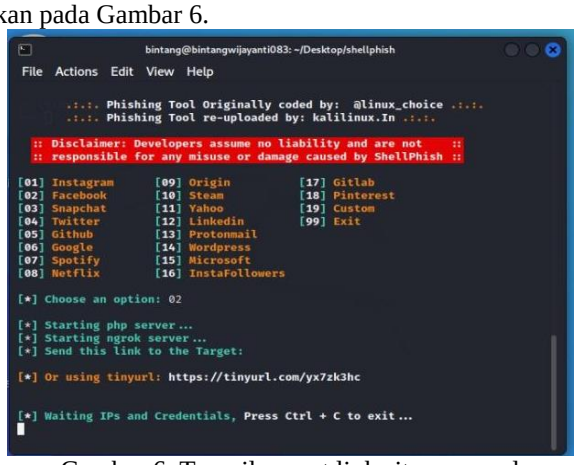
Pada pengujian pada *tools shellphish* yang kami kerjakan, terdapat beberapa tahapan dan hasil akhir dalam menjalankan *tools* ini, yaitu sebagai berikut.

1. Setelah menginstal *tools shellphish* pada kali linux, tampilan selanjutnya adalah tampilan halaman situs populer untuk melakukan tindakan phishing yang ditunjukkan pada Gambar 5.



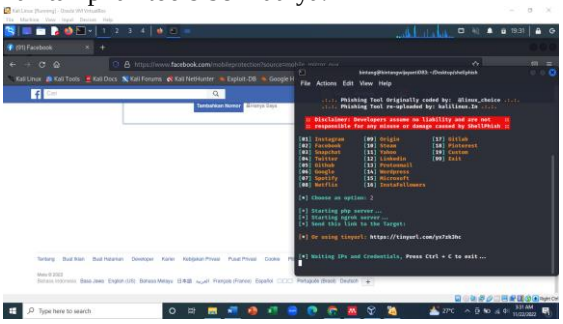
Gambar 5. Tampilan halaman situs pada shellphish

2. Setelah memilih opsi salah satu dari situs populer tersebut, tampilan selanjutnya adalah muncul sebuah *link phising* yang nantinya akan diberikan kepada target seperti ditunjukkan pada Gambar 6.



Gambar 6. Tampilan saat link situs muncul

3. Setelah target membuka link, kita dapat melihat IP dan *Password* korban. Gambar 7 menunjukkan tampilan *tools* berikutnya.



Gambar 7. Tampilan saat link dibuka

c. *WhPhisher*

- Analisis

WhPhisher merupakan salah satu *tools* terbaik untuk melakukan *phising* dengan halaman yang paling terkenal yang telah diperbarui[7]. *WhPhisher* telah diuji pada Termux, Debian dan pada Kali Linux[7]. Namun untuk membuat tools ini lebih kecil kemungkinan gagal, disarankan untuk menginstall Termux versi terbaru dan Termux API[7].

- Pengukuran

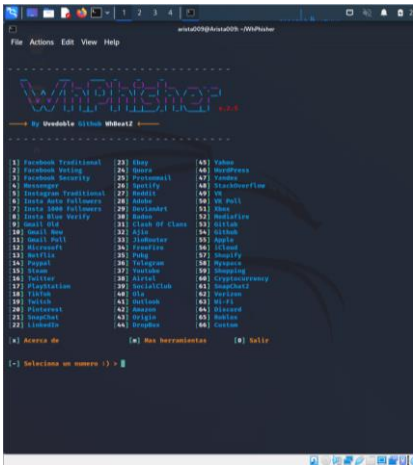
Pengukuran pada tools *WhPhisher* ini terdapat pada percobaan phising yang telah dilakukan. *Tools* ini tidak dapat bekerja secara efektif dalam menampilkan opsi laman facebook. Penginstalan yang dilakukan juga

dapat dikatakan lebih lama dibanding *Zphisher* dan *Shellphish*. Untuk menjalankan *tools* ini memerlukan waktu 1 menit 12 detik dan hanya diperlukan 2 langkah untuk mendapatkan *link* akses tersebut. Dari 6 kali percobaan yang telah dilakukan terhadap berbagai opsi target *phising* menggunakan *WhPhisher* ini tidak dapat memunculkan *link* yang relevan dengan opsi yang diberikan. Salah satu contohnya adalah ketika memilih opsi "*facebook traditional*" dimana *link* yang muncul adalah *link* mengenai verifikasi *facebook*.

- Pengujian

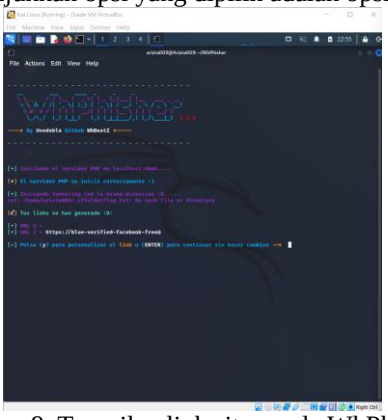
Berikut ini merupakan tahapan menggunakan *WhPhisher*.

1.Langkah pertama adalah melakukan instalasi *tools WhPhisher* pada Kali Linux. Gambar 8 menunjukkan tampilan *WhPhisher* setelah instalasi selesai.



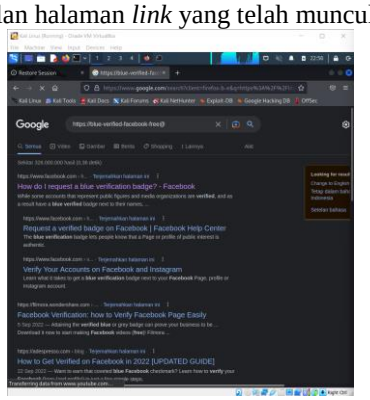
Gambar 8. Tampilan WhPhisher

2.Setelah melakukan instalasi *tools WhPhisher* pada Kali Linux, selanjutnya adalah memilih opsi salah satu dari berbagai opsi. Gambar 9 menunjukkan opsi yang dipilih adalah opsi 1 yaitu *facebook traditional*.



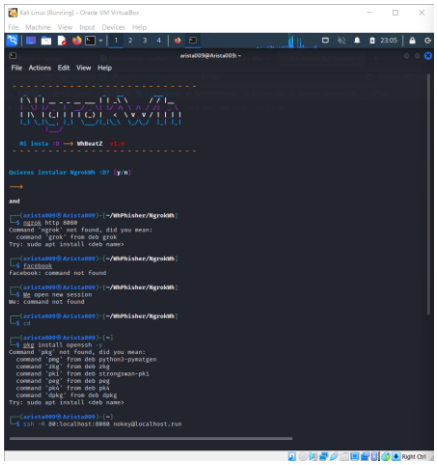
Gambar 9. Tampilan link situs pada WhPhisher

3.Setelah memilih opsi 1 tersebut lalu *enter*, selanjutnya akan muncul adalah proses dalam memunculkan *link*. Gambar 10 menunjukkan tampilan halaman *link* yang telah muncul.



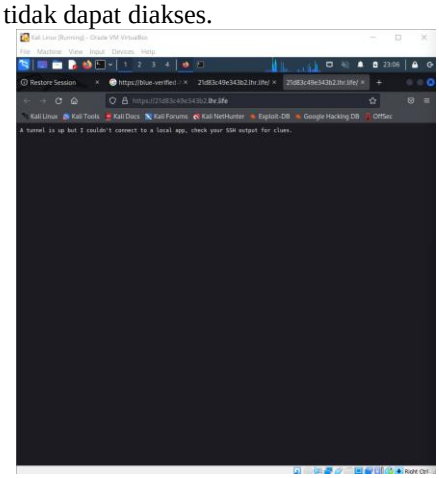
Gambar 10. Tampilan ketika link di klik

4.Setelah membuka *link*, halaman yang muncul harusnya adalah halaman mengenai opsi yang telah dipilih. Akibat *link* yang muncul tidak sesuai, maka dilakukan cara lain untuk mendapatkan *link facebook* yang diinginkan yang ditunjukkan pada Gambar 11.



Gambar 11. Tampilan *NgrokWh*

5.Namun *link* tetap tidak muncul dan pencarian selesai karena tidak menemukan jalan lain. Gambar 12 dibawah menunjukkan *link* yang tidak dapat diakses.



Gambar 12. Tampilan link yang diberikan *NgrokWh*

4. HASIL DAN PEMBAHASAN

a. Proses *Cloning Website* aplikasi facebook menggunakan *Tool Zphisher*

Pada *tool Zphisher* dipilih *template* no. 1 yaitu facebook untuk selanjutnya memilih menu *Localhost* untuk selanjutnya membuat/menampilkan link URL yang nantinya akan diberikan kepada korban. Tampilan seperti pada gambar dibawah ini.

Gambar 13. Tampilan link ZPhisher

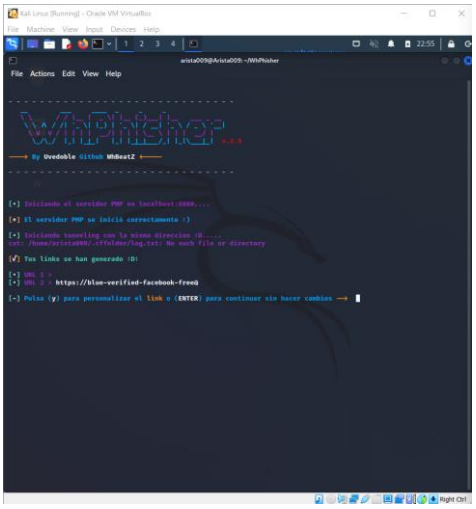
b. Proses *Cloning Website* aplikasi facebook menggunakan *Tool shellphish*

pada *tool Shellphish* dipilih *template* no. 2 yaitu facebook untuk selanjutnya membuat *cloning website* menggunakan link URL yang nantinya diberikan kepada korban. tampilan seperti pada gambar dibawah ini.

Gambar 14. Tampilan link Shellphish

c. Proses *Cloning Website* aplikasi facebook menggunakan *Tools WhPhisher*.

Pada tools *WhPhisher* memilih opsi 1 dengan keterangan *facebook tradisional* yang kemudian membuat cloning *website* menggunakan *link URL* yang diberikan. Gambar 1 menunjukkan tampilan tampilan *link* yang muncul.



Gambar 15. Tampilan link WhPhisher

3.2 Tabel Hasil Perbandingan

Tabel 1 Perbandingan tiga *tools phising* yang di analisis yaitu *ZPhisher*, *Shellphish* dan *WhPhisher*.

Nama Tools	Durasi	Efektivitas
ZPhisher	14 detik	Efektif
Shellphish	24 detik	Kurang Efektif
WhPhisher	1 menit 12 detik	Tidak Efektif

Tabel 1. Hasil perbandingan 3 tools

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis yang telah dilakukan, maka dapat disimpulkan bahwa hasil penelitian dari kelompok kami terkait dengan *tools phishing* yang kami gunakan yakni diantaranya, *Zphisher*, *Shellphish* dan *Whphisher*, mendapatkan hasil yang tentu berbeda-beda. Hal ini dikarenakan pada masing-masing *tools* yang memiliki respon yang berbeda dan proses yang berbeda. Analisis kerentanan kejahatan online dari tiga *tools phising* yang digunakan memiliki perbedaan tersendiri. *Tools* pertama yaitu *Zphisher* dapat dikatakan paling efektif dalam melakukan *phising* dari dua *tools* lainnya. Hal ini dapat dilihat dari kecepatan akses instalasi, akurasi dan efektivitasnya. Maka dari tiga *tools* yang dianalisis, satu *tools* dapat dikatakan efektif penggunaannya.

Ucapan Terima Kasih
Puji dan syukur kami panjatkan kepada Tuhan Yang Maha Esa, karena berkat rahmat-Nya, kami dapat menyelesaikan artikel ini. Penulisan artikel ini dilakukan dalam rangka memenuhi salah satu syarat untuk ujian akhir semester. Kami menyadari, tanpa bantuan dan bimbingan dari berbagai pihak, cukup sulit bagi kami dalam menyelesaikan artikel ini. Kami menyadari dalam penulisan artikel ini masih terdapat kekurangan, maka diharapkan kritik dan saran yang membangun untuk menyempurnakan artikel ini.

DAFTAR PUSTAKA

[1] S. Wahyuni, I. M. Raazi, dan D. I. Dwitawati, "Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 5, no. 1, hlm. 49–55, Feb 2022, Diakses: Nov 23, 2022. [Daring]. Available: https://ojs.serambimekkah.ac.id/jnkti/article/view/3962

[2] "16917211 Kun Saidi".

[3] K. Saidi dan Y. Prayudi, "Analisis Indikator Utama Dalam Information Security-Personality Threat Terhadap Phishing Attack Menggunakan Metode Technology Threat Avoidance Theory (TTAT)".

[4] "ZPhisher -- Advanced Lazy Automated Phishing Script." https://www.kalilinux.in/2020/03/zphisher-phishing-kali-linux-2020.html (diakses Nov 24, 2022).

[5] J. H. Moedjahedy, A. Setyanto, dan K. Aryasa, "ANALISIS PERBANDINGAN KORELASI SPEARMAN DAN MAXIMAL INFORMATION COEFFICIENT DALAM SELEKSI FITUR WEBSITE PHISHING MENGGUNAKAN ALGORITMA MACHINE LEARNING," *CSRID (Computer Science Research and Its Development Journal)*, vol. 12, no. 2, hlm. 107, Mar 2021, doi: 10.22303/csrid.12.2.2020.107-116.

[6] "Shellphish -- Simple Phishing Toolkit | Phishing Page Creator." https://www.kalilinux.in/2019/04/shellphish-phishing-page-creator.html (diakses Nov 24, 2022).

[7] "GitHub - WhBeatZ/WhPhisher: The best tool for phishing on Termux / Linux, 2022 updated. Programed by The Famous Sensei." https://github.com/WhBeatZ/WhPhisher (diakses Nov 24, 2022).