INFOTECH journal
ISSN : 2460-1861 (Print), 2615-4250 (Online)
Vol. 10 No. 2 Desember 2024, pp. 297-305

ANALISIS DAMPAK ANCAMAN CYBERCRIME TERHADAP DATA MAHASISWA PADA SERANGAN WEB PHISING SIAK UIKA

Berlyan Gumay[1], Ade Hendri Hendrawan[2], Fitrah Satrya Fajar Kusumah[3]
[1,2,3]Teknik Informatika, Fakultas Teknik dan Sains, Universitas Ibn Khaldun
Email: berlyan5268@gmail.com

ABSTRACT
The rapid development of information technology has significantly increased global connectivity and efficiency, but it has also heightened the risk of cybercrime, including phishing. Phishing is a form of cyberattack that deceives individuals into revealing sensitive information, such as passwords or personal details, by disguising malicious intent. This study employs quantitative methods to assess the impact of phishing attacks on second-semester students of the Informatics Engineering Study Program at Ibn Khaldun University Bogor. It also evaluates the students' cybersecurity awareness levels. Data were collected from 107 students who served as the research sample. The findings indicate that 54 students accessed phishing sites, resulting in 30 instances of valid usernames and passwords being compromised, representing 28% of the sample. This percentage falls into the low-awareness category. These results underscore the need for enhanced cybersecurity education among university students to prevent future phishing attacks. This research contributes valuable insights into student behavior in the face of cybercrime threats.

Keywords Information technology, Phishing, Cybercrime,Cybersecurity, Setoolkit, Social Engineering.

ABSTRAK
Perkembangan teknologi informasi yang pesat telah meningkatkan konektivitas dan efisiensi global secara signifikan, tetapi juga meningkatkan risiko kejahatan dunia maya, termasuk phishing. Phishing adalah bentuk serangan siber yang menipu individu untuk mengungkapkan informasi sensitif, seperti kata sandi atau detail pribadi, dengan menyamarkan niat jahat. Penelitian ini menggunakan metode kuantitatif untuk menilai dampak serangan phishing terhadap mahasiswa semester dua Program Studi Teknik Informatika Universitas Ibn Khaldun Bogor. Penelitian ini juga mengevaluasi tingkat kesadaran keamanan siber mahasiswa. Data dikumpulkan dari 107 mahasiswa yang menjadi sampel penelitian. Temuan menunjukkan bahwa 54 mahasiswa mengakses situs phishing, yang mengakibatkan 30 contoh nama pengguna dan kata sandi yang valid dibobol, mewakili 28% dari sampel. Persentase ini termasuk dalam kategori kesadaran rendah. Hasil ini menggaris bawahi perlunya peningkatan pendidikan keamanan siber di kalangan mahasiswa untuk mencegah serangan phishing di masa depan. Penelitian ini memberikan kontribusi wawasan yang berharga tentang perilaku mahasiswa dalam menghadapi ancaman kejahatan siber.

Kata Kunci: *Teknologi Informasi, Phising, Kejahatan Siber, Keamanan Siber, Setoolkit, Rekayasa Sosial.*

Riwayat Artikel :

Tanggal diterima : 04-10-2024

Tanggal revisi : 07-10-2024

Tanggal terbit : 13-10-2024

DOI :

https://doi.org/10.31949/infotech.v10i2.11463

1. PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi telah memberikan manfaat besar dalam kehidupan sehari-hari, namun juga memunculkan ancaman serius berupa kejahatan siber atau *cybercrime* (Nofiyan and Mushlihudin 2020). Cybercrime adalah sebuah kejahatan yang menggunakan sumber daya jaringan (internet) guna mencapai tujuan ilegal seperti mencuri data, penipuan dan pelanggaran privasi (Ubaidillah, Dani Noval Kurnia, and Ruth Vanya Octaviany 2022). Salah satu bentuk *cybercrime* yang mengkhawatirkan adalah serangan phishing, di mana penyerang memanipulasi korban untuk mendapatkan informasi sensitif melalui taktik yang menyamar sebagai entitas terpercaya (Alkhalil 2021). Ancaman phising dapat mengakibatkan kerugian finansial, pencurian identitas, serta kerusakan reputasi (Kheruddin, 2024). Berdasarkan laporan dari organisasi internasional Anti-Phishing Working Group (APWG), tercatat lebih dari 4,7 juta serangan phishing terjadi sepanjang tahun 2022, dengan peningkatan sekitar 150% per tahun sejak awal 2019. Banyak korban dari serangan phishing ini mengalami kerugian signifikan, terutama terkait privasi, seperti pencurian data dan penyalahgunaan informasi, serta kerugian finansial yang tidak sedikit. Serangan phishing yang dilakukan oleh para cracker bertujuan untuk mendapatkan informasi sensitif, seperti nama pengguna, kata sandi, dan detail kartu kredit, dengan menyamar sebagai pihak yang terpercaya, seperti otoritas resmi, administrator sistem, pegawai pemerintahan, atau organisasi sah. Biasanya, serangan ini dilakukan melalui komunikasi elektronik, dalam bentuk permintaan untuk memperbarui informasi akun yang menjadi target (Permata and Ratnawati 2023).

Rekayasa sosial merupakan suatu metode di mana para penipu atau penyerang memanipulasi korban guna memperoleh informasi rahasia atau mendapatkan akses ke dalam sebuah sistem komputer (Ahmadian and Sabri 2021). Maka dari itu pentingnya keamanan informasi pribadi di era serangan siber, keamanan informasi adalah serangkaian praktik, kebijakan, prosedur, dan teknologi yang bertujuan melindungi integritas, kerahasiaan, dan ketersediaan informasi (Nurbojatmiko 2024).

Keamanan informasi memastikan bahwa data, sistem, dan sumber daya terkait tetap aman dari ancaman, kerentanan, atau serangan yang dapat membahayakan keberlanjutan, nilai, dan kepercayaan informasi (Arie 2021). Penelitian ini bertujuan untuk menganalisis dampak ancaman *cybercrime*, khususnya serangan *phishing*, terhadap data mahasiswa pada serangan web *phishing* SIAK palsu di kalangan mahasiswa semester 2 Program Studi Teknik Informatika. Penelitian ini juga mengevaluasi tingkat kesadaran dan kehati-hatian mahasiswa terhadap serangan *phishing*, serta mengidentifikasi faktor-faktor yang memengaruhi perilaku keamanan mereka. bermanfaat dalam menjaga keamanan informasi pribadi.

1.2. Tinjuan Pustaka

1. Kali Linux

Kali Linux (H. S. Harahap et al. 2024) adalah distribusi berbasis Debian GNU/Linux yang dirancang khusus untuk keperluan forensik digital dan pengujian penetrasi. Distribusi ini dikelola dan didanai oleh Offensive Security. Kali Linux dikembangkan oleh Mati Aharoni, yang sebelumnya terlibat dalam pengembangan Backtrack, bersama dengan Devon Kearns dari Offensive Security.

2. Setoolkit

Setoolkit adalah (Syafitri et al. 2022) rangkaian alat yang digunakan untuk melakukan serangan *social engineering*, yang memanipulasi korban untuk mendapatkan akses tidak sah ke dalam sistem, informasi *sensitive*, atau kredensial pengguna. berbagai jenis serangan, seperti *phising*, pembuatan situs *web* palsu dan serangan lainya yang memanfaatkan kelemahan korban dalam proses keamanan informasi.

3. Web Phising

Web phishing adalah bentuk serangan siber yang melibatkan upaya untuk memanfaatkan situs *web* palsu dengan tujuan mengelabui korban (Yurita et al. 2023). Dalam praktiknya, situs *web phising* di desain sedemikian rupa sehingga secara tampilan sangat menyerupai situs resmi yang sah, seringkali menggunakan nama *domain* yang sangat mirip. Fenomena ini, dikenal sebagai *domain spoofing*, menciptakan ilusi keaslian dan meyakinkan pengguna untuk memasukkan informasi sensitif seperti kata sandi, rincian keuangan, atau data pribadi lainnya. Dengan memanfaatkan kecurigaan rendah pengguna terhadap situs *web* yang tampak serupa dengan yang sah, para penyerang berusaha mencapai tujuan kriminal mereka, menimbulkan risiko keamanan informasi yang serius (Fanasafa 2022).

4. Rekayasa Sosial

Rekayasa sosial (Ahmadian & Sabri 2021) merupakan suatu metode di mana para penipu atau penyerang memanipulasi korban guna memperoleh informasi rahasia atau mendapatkan akses ke dalam sebuah sistem komputer. Berbeda dengan serangan yang mengandalkan kerentanan teknis, rekayasa sosial fokus pada eksploitasi sifat alami manusia, seperti kepercayaan, ketidakcurigaan, dan keinginan untuk membantu. Dengan menggunakan interaksi sosial, penyerang berusaha memanipulasi korbannya agar melakukan tindakan yang menguntungkan penyerang, membuka pintu bagi potensi kebocoran informasi atau akses ilegal ke sebuah sistem.

5. *Ngrok*

Ngrok (Parlika et al. 2020) adalah sebuah perangkat lunak yang memungkinkan Anda membuat terowongan (tunnel) aman dari internet ke komputer lokal Anda. Ini berarti Anda dapat memberikan akses ke server lokal Anda melalui internet, bahkan jika server Anda berada di belakang firewall atau router yang rumit. Ngrok biasanya digunakan untuk tujuan pengembangan dan pengujian aplikasi web lokal, serta untuk berbagi akses ke server lokal dengan rekan kerja atau klien tanpa harus mengekspos server langsung ke internet.

6. Keamanan Informasi

Keamanan informasi adalah serangkaian praktik, kebijakan, prosedur, dan teknologi yang bertujuan melindungi integritas, kerahasiaan, dan ketersediaan informasi. Keamanan informasi memastikan bahwa data, sistem, dan sumber daya terkait tetap aman dari ancaman, kerentanan, atau serangan yang dapat membahayakan keberlanjutan, nilai, dan kepercayaan informasi. Ini melibatkan menjaga integritas informasi agar tidak diubah oleh pihak yang tidak berwenang dan memastikan bahwa hanya pihak yang berwenang yang memiliki akses ke informasi tersebut. Keamanan informasi juga mencakup pelacakan dan otentikasi setiap modifikasi informasi serta menjaga kerahasiaan data agar tidak dapat diakses oleh pihak yang tidak berhak. Dengan pendekatan holistik ini, keamanan informasi menciptakan lingkungan yang dapat melindungi informasi dari berbagai ancaman dan risiko yang mungkin timbul, 3 aspek keamanan informasi (Arie, Suprio, dan Najib n.d.). Keamanan informasi dapat dilihat pada gambar 1.

Gambar 1 Keamanan Informasi

6.1 *Confidentiality*

Keamanan informasi dari sudut pandang kerahasiaan (*Confidentiality*) berfokus pada perlindungan informasi sensitif dari akses atau pengungkapan yang tidak sah. Hal ini mencakup penerapan enkripsi, pengaturan hak akses yang ketat, manajemen identitas, pemantauan aktivitas, klasifikasi data, serta pelatihan pengguna untuk menjaga kerahasiaan informasi.

6.2 *Integrity*

Keamanan informasi dari aspek integritas (Integrity) bertujuan untuk memastikan bahwa data tetap utuh dan tidak mengalami perubahan yang tidak sah. Upaya ini mencakup pengendalian akses, penggunaan tanda tangan digital, pengelolaan versi, audit, serta penerapan enkripsi untuk menjaga integritas data.

6.3 *Availability*

Keamanan informasi dari aspek ketersediaan (Availability) bertujuan untuk memastikan bahwa sistem, data, dan layanan tetap dapat diakses oleh pengguna yang sah saat diperlukan. Upaya ini melibatkan penerapan redundansi, pencegahan serangan, manajemen kapasitas, pemulihan bencana, pemantauan, serta pemeliharaan sistem secara rutin (A. H. Harahap et al. 2023).

7. Metode Perhitungan

Metode Perhitungan Responden (Rosnidar, Zulfan, and Nurasiah 2020) adalah teknik untuk menyajikan data dalam bentuk proporsi dari nilai keseluruhan. Responden digunakan untuk memudahkan perbandingan antara berbagai bagian atau untuk menunjukkan bagian relatif dari suatu total nilai tersebut untuk metode perhitungan yang digunakan dapat dilihat pada tabel 1.

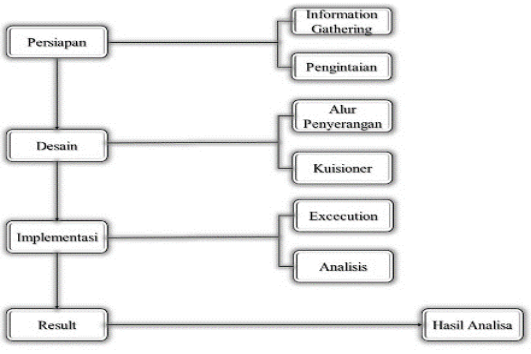
Tabel 1. Metode Perhitungan

No	Skor Siswa	Kategori Sikap
1	$x \geq (\bar{x} + SBx)$	Sangat positif/sangat tinggi
2	$(\bar{x} + SBx) > x \geq \bar{x}$	Positif/tinggi
3	$\bar{x} > x \geq (\bar{x} - SBx)$	Negatif/rendah
4	$x < (\bar{x} - SBx)$	Sangat negatif/rendah

Keterangan:
$\bar{x}$ = rata-rata skor keseluruhan
SBx = simpangan baku
x = skor yang dicapai siswa

1.3. Metodologi Penelitian

Metode penelitian yang dilakukan pada penelitian ini berupa kerangka kerja untuk melakukan suatu tindakan atau kerangka berfikir untuk menyusun suatu gagasan terarah dan terkait dengan maksud dan tujuan. Adapun tahapan-tahapan atau kerangka berfikir yang dilakukan pada metode penelitian ini dapat dilihat pada gambar 2.



Gambar 2 Alur Penelitian

1. Persiapan

1.1 Information Gathering

Pengumpulan informasi adalah dimana penyerang mengumpulkan informasi tentang target potensial. Melibatkan identifikasi data yang relevan, Pengumpulan informasi adalah dimana penyerang mengumpulkan informasi tentang target potensial. Melibatkan identifikasi data yang relevan, seperti alamat email, hanphone atau informasi lainya yang dapat digunakan untuk meningkatkan keberhasilan serangan phising.

1.2 Pengintaian

Pengintaian tahap dimana penyerang menarik perhatian korban dan memancing korban agar memberikan inforrmasi sensitif atau melakukan tindakan yang merugikan, seperti mengklik tautan berbahaya atau memberikan informasi data pribadi kepada si penyerang.

2. Desain

2.1 Alur Penyerangan

Tujuan dari alur penyrangan ini adalah untuk memberitahukan bagaimana skema penyerangan yang akan digunakan dalam penelitian tersebut.

2.2 Kuisioner

Tujuan adanya kuisioner adalah memberikan pemahaman wawasan tentang tingkat pemahaman dan kesadaran mahasiswa terhadap ancaman *phising*, guna mengidentifikasi perilaku mahasiswa dalam menjaga informasi data pribadi.

3. Implementasi

3.1 Excecution

Pada tahap ini dimana penyerang melaksanan serangan, seperti mencuri informasi *login*, mengirimkan tautan situs *web* palsu, setelah korban terpengaruh dan memberikan informasi pribadi atau melaksanan tindakan yang diminta.

3.2 Analisis

Pada tahap Analisis ini kita menghitung berapa banyak mahasiswa yang terjebak terhadap serangan *web phising* dalam menjaga keamanan data pribadi.

4. Result

4.1 Hasil Analisa

Tahap terakhir merupakan tahap hasil. Dimana dalam tahap ini terdapat berapa banyak mahasiswa yang terkena serangan *web phising*, serta mengetahui jumlah mahasiswa mana yang paling banyak terjebak dalam serangan tersebut.

2. PEMBAHASAN

2.1 Sampel Penelitian

Data jumlah mahasiswa semester 2 program studi Teknik Informatika, sebanyak 107 mahasiswa. Diantaranya dapat dilihat pada tabel 2.

Tabel 2. Sampel Penelitian

Keterangan	Jumlah
Laki - Laki	91
Perempuan	16

2.2 Data Kuisioner

Terdapat beberapa pertanyaan yang dibuat dalam penelitian kali ini yang menggunakan kuisioner sebagai acuan untuk mengetahui Tingkat kesadaran mahasiswa dalam menjaga data pribadi terhadap serangan web *phising.*

1. Seberapa sering Anda menggunakan kata sandi yang kuat dan unik untuk akun online Anda?
2. Seberapa sering Anda memeriksa tautan pendek atau URL yang disingkat sebelum mengaksesnya?
3. Seberapa sering Anda mencurigai tautan eksternal dalam email atau pesan online sebelum mengkliknya?
4. Apakah Anda sering memperhatikan security akses sebelum memasuki sebuah *web*?
5. Apakah Anda pernah menerima email atau pesan yang mencurigakan yang mencoba meminta informasi pribadi Anda seperti kata sandi atau *Username*?
6. Apakah Anda pernah menjadi korban serangan *web phishing*, di mana informasi pribadi Anda telah disalahgunakan secara online?
7. Apakah Anda pernah memikirkan dampak negatif sebelum memposting sesuatu pada media sosial?
8. Apakah Anda pernah membagikan informasi pribadi Anda secara tidak sengaja melalui situs *web* palsu yang terlihat seperti situs *web* resmi yang Anda percayai?
9. Apakah Anda pernah tergoda untuk mengklik tautan yang disertakan dalam email yang mencurigakan?
10. Apakah Anda pernah mengklik *link*, *thumbnail* ataupun tautan pada pesan *link*, hanya jika itu berasal dari orang yang saya kenal?

Berdasarkan pertanyaan di atas terbagi menjadi 4 kategori jawaban yang digunakan sebagai landasan peneliti untuk mengetahui aspek pengetahuan dan Tingkat kesadaran mahasiswa diantaranya: Sering, Kadang-Kadang, Jarang dan Tidak Pernah.

a. Dari hasil pertanyaan pertama menujukan bahwa mahasiswa yang menjawab Sering sebesar 57,6%, Kadang-Kadang 29,3%, Jarang 10,9% sedangkan Tidak Pernah sebanyak 2,2%.

Gambar 3. Pertanyaan 1

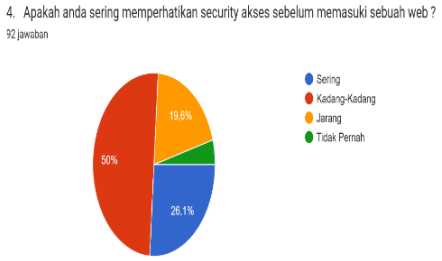
b. Dari hasil pertanyaan Kedua menujukan bahwa mahasiswa yang menjawab Sering sebesar 21,7%, Kadang-Kadang 38%, Jarang 30,4%, Tidak Pernah sebanyak 9,8% sedangkan tidak menjawab 1,1%.

Gambar 4. Pertanyaan 2

c. Dari hasil pertanyaan ketiga menujukan bahwa mahasiswa yang menjawab Sering sebesar 52,2%, Kadang-Kadang 30,4%, Jarang 16,3% sedangkan Tidak Pernah sebanyak 1,1%.

Gambar 5. Pertanyaan 3

d. Dari hasil pertanyaan keempat menujukan bahwa mahasiswa yang menjawab Sering sebesar 26,1%, Kadang-Kadang 50%, Jarang 19,6% sedangkan Tidak Pernah sebanyak 4,3%.



Gambar 6. Pertanyaan 4

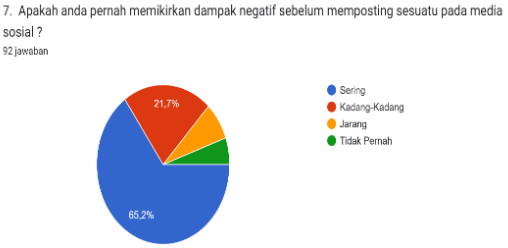
e. Dari hasil pertanyaan kelima menujukan bahwa mahasiswa yang menjawab Sering sebesar 12%, Kadang-Kadang 23,9%, Jarang 38% sedangkan Tidak Pernah sebanyak 26,1%.

Gambar 7. Pertanyaan 5

f. Dari hasil pertanyaan keenam menujukan bahwa mahasiswa yang menjawab Sering sebesar 6,5%, Kadang-Kadang 17,4%, Jarang 17,4% sedangkan Tidak Pernah sebanyak 58,7%.

Gambar 8. Pertanyaan 6

g. Dari hasil pertanyaan ketujuh menujukan bahwa mahasiswa yang menjawab Sering sebesar 65,2%, Kadang-Kadang 21,7%, Jarang 7,6% sedangkan Tidak Pernah sebanyak 5,4%.



Gambar 9. Pertanyaan 7

h. Dari hasil pertanyaan ketujuh menujukan bahwa mahasiswa yang menjawab Sering sebesar 65,2%, Kadang-Kadang 21,7%, Jarang 7,6% sedangkan Tidak Pernah sebanyak 5,4%.

Gambar 10. Pertanyaan 8

i. Dari hasil pertanyaan ke Sembilan menujukan bahwa mahasiswa yang menjawab Sering sebesar 8,7%, Kadang-Kadang 26,1%, Jarang 15,2% sedangkan Tidak Pernah sebanyak 50%.

Gambar 11. Pertanyaan 9

j. Dari pertanyaan ke sepuluh menujukan bahwa mahasiswa yang menjawab Sering sebesar 37%, Kadang-Kadang 30,4%, Jarang 19,6% sedangkan Tidak Pernah sebanyak 13%.

Gambar 12. Pertanyaan 10

Tabel 3 Tingkat Kategori Mahasiswa yang Terkena Serangan Phising.

Keterangan	Persentase
Sangat Rendah	0–20%
Rendah	21-40 %
Sedang	41–60%
Tinggi	61–80%
Sangat Tinggi	81–100%

2.3 Metode Perhitungan

Metode yang digunakan dalam penelitian kali ini menggunakan Teknik persentase dengan rumus sebagai berikut:

P = F/n x 100%

Keterangan :

P = besaran persentase

F = frekuensi jawaban

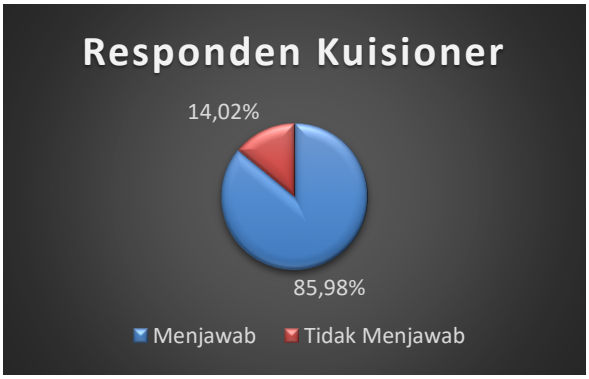
N = jumlah responden

Setelah nilai dihitung dalam bentuk persentase, hasil tersebut kemudian dimasukkan ke dalam kriteria penilaian persentase.

Berdasarkan data mahasiswa yang masuk ke dalam situs web *phising* yang digunakan untuk mengetahui akan dampak terjadinya ketika serangan *cybercrime* khususnya *phising* terhadap mahasiswa sebanyak 30 data yang valid 54 mahasiswa yang masuk ke dalam web phising dari total keseluruhan mahasiswa sebanyak 107. Berikut hasil persentase di jelaskan pada gambar 13.

$$\frac{Jumlah\ Responden}{Total\ Responden} X\ Persentase\ (100\%) = \frac{92\ Mahasiswa}{107\ Mahasiswa}\ X\ 100\ \% = 85{,}98\%$$ Yang Menjawab Kuisioner

$$\frac{Jumlah\ Responden}{Total\ Responden} X\ Persentase\ (100\%) = \frac{15\ Mahasiswa}{107\ Mahasiswa}\ X\ 100\ \% = 14{,}02\%$$ yang Tidak Menjawab Kuisioner

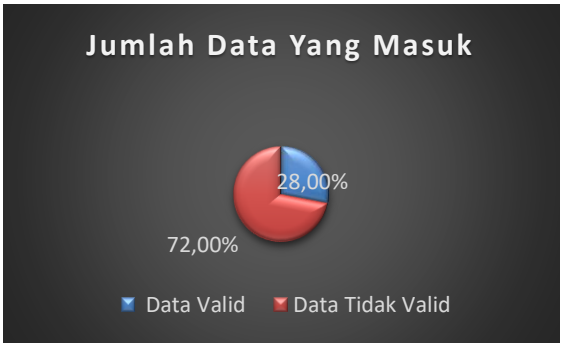


Gambar 13. Responden Kuisioner

Gambar 14. Serangan Phising

Sedangkan mahasiswa yang terkena serangan *phising* sebanyak : $\frac{Jumlah\ Responden}{Total\ Responden} X\ Persentase\ (100\%)$ = $\frac{54\ Mahasiswa}{107\ Mahasiswa} X\ 100\ \% = 50{,}47\ \%$ Yang Tekena Serangan *Phising*.

Sedangkan mahasiswa yang tidak terkena serangan *phising* sebanyak : $\frac{Jumlah\ Responden}{Total\ Responden} X\ Persentase\ (100\%)$ = $\frac{53\ Mahasiswa}{107\ Mahasiswa} X\ 100\ \% = 49{,}53\ \%$ Yang Tidak Terkena Serangan *Phising*.



Gambar 15. Jumlah Data Yang Masuk

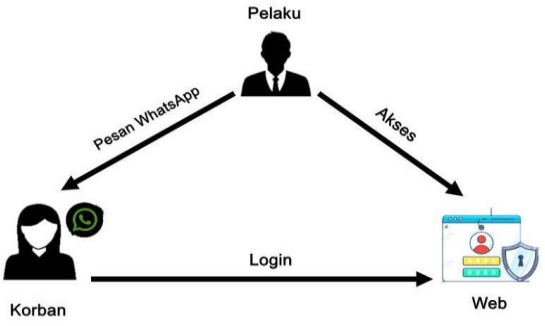
Berdasarkan data yang masuk ke dalam sebuah sistem dan telah di report ke dalam bentuk txt, sebanyak 54 *username* dan *password*, sedangkan yang valid sebanyak 30 *username password* yang telah di lakukan pengujian satu per satu, dan yg tidak valid sebanyak 24 *username password* dari total 107 mahasiswa.

jadi dapat disimpulkan bahwa jumlah data yang masuk adalah : $\frac{Jumlah\ Data\ Masuk}{Data\ Valid} X\ Persentase\ (100\%)$ = $\frac{30\ Mahasiswa}{107\ Mahasiswa} X\ 100\ \% = 28\%$ Jumlah Data Yang Valid

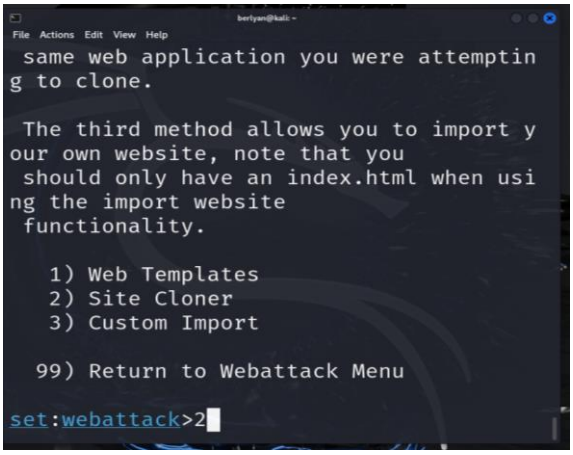
jadi dapat disimpulkan bahwa jumlah data yang masuk adalah : $\frac{Jumlah\ Data\ Masuk}{Data\ Tidak\ Valid} X\ Persentase\ (100\%)$ = $\frac{77\ Mahasiswa}{107\ Mahasiswa} X\ 100\ \% = 72\%$ Jumlah Data Yang Tidak Valid

2.4 Tahapan Percobaan

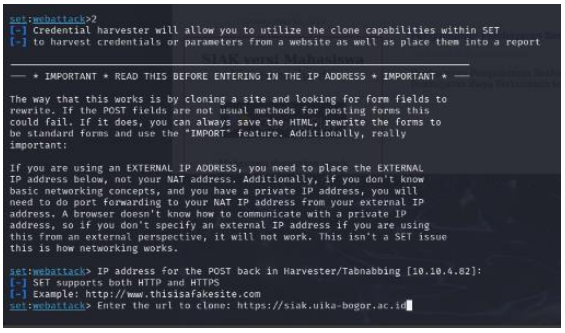
Dalam percobaan kali ini penulis melakukan serangan *phising* menggunakan setoolkit yang digunakan untuk meng-*clonning* sebuah website, kemudian digunakan target untuk login menggunakan username dan password, maka target akan di redirect bahwa ia telah mengirimkan ke situs aslinya tanpa menyadari bahwa ia telah mengirimkana kredensial kepada penyerang.



Gambar 16. Alur Penyerangan



Gambar 17. Tahapan Persiapan Setoolkit



Gambar 18. Clonning Website

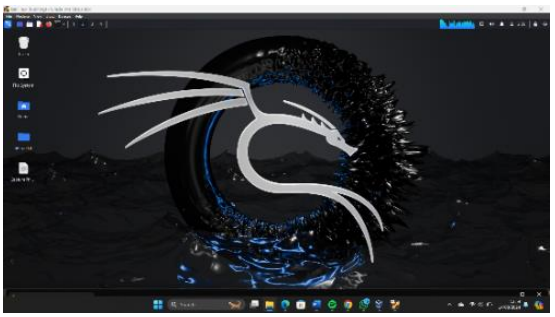
2.5 Proses Pesan Phising Setoolkit

Penyerang mengirimkan pesan *whatsapp* kepada korban berupa sebuah tautan palsu dengan menyamar sebagai entitas terpecaya dengan tujuan mendapatkan akses pribadi berupa *username* dan *password.*

Gambar 19. Pesan Phising

Setelah target menerima pesan yang dikirimkan oleh penyerang, maka target akan dibawa ke halaman web palsu yang menyerupai aslinya. Selanjutnya target melakukan login ke halaman tersebut. Kemudian data yang di dapat akan di simpan di dalam file Txt.

Gambar 20. Halaman Clonning Web Phising



Gambar 21. Hasil Kredensial

3 KESIMPULAN

Berdasarkan dari hasil pembahasan yang telah dilakukan *Social Engineering* adalah sebuah Teknik yang digunakan sebagai media pendekatan kepada korban untuk mengelabui sisi kelemahan yang menjadi celah terjadinya pencurian informasi. Dengan demikian hasil penelitian ini menyimpulkan terdapat 54 mahasiswa yang masuk ke dalam sebuah tautan palsu, sedangkan data yang valid sebanyak 30 *username password* yang di dapat oleh penyerang berdasarkan kategori persentase di atas menyimpulkan bahwa masih dalam kategori rendah yang artinya 28 % mahasiswa yang terkena serangan phising berdasarkan data yang valid. Akan tetapi kedepan nya agar dapat memperhatikan tautan situs web dan security dalam mengakses sebuah situs yang akan dikunjungi.

PUSTAKA

Ahmadian, Hendri, and Aulia Sabri. 2021. "Teknik Penyerangan Phishing Pada Social Engineering Menggunakan Set Dan Pencegahannya." *Djtechno Jurnal Teknologi Informasi* 2(1): 13–20.

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. 2021. "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy." *Frontiers in Computer Science* 3(March): 1–23.

Arie, Yoyon, Budi Suprio, and Moch Najib. "Analisa Dampak Kesadaran Keamanan Informasi Pengguna Aplikasi Whatsapp Terhadap Penyebaran Link Web Phising, 11 AGUSTUS 2022." *SEMINAR NASIONAL CORISINDO*.

Fanasafa, Irfan. 2022. "Waspada! Kehajatan Phising Mengintai Anda." *https://www.djkn.kemenkeu.go.id*. https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html (January 23, 2023).

Harahap, Abdul Halim et al. 2023. "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi Dan Data Untuk Pemangku Kepentingan Atau Stakholder." *Jurnal Manajemen dan Pemasaran Digital* 1(2): 73–83.

Harahap, Handika Saputra, Allegra Alif Rahman, Indah Suraswati, and Shelvie Nidya Neyman. 2024. "Memahami Cara Kerja Phishing Menggunakan Tools Pada Kali Linux." (2): 1–11.

Kheruddin, Muhammad Syafiq et al. 2024. "Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape." *Advance.Sagepub.Com*. https://advance.sagepub.com/doi/full/10.22541/au.170534654.48067877/v1.

Nofiyan, Agil, and Mushlihudin Mushlihudin. 2020. "Analisis Forensik Pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)." *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)* 8(2): 53.

Nurbojatmiko, Nurbojatmiko, Muhammad Shidqa Irahman, Ainun Nashikha, and Raihan Lail Ramadhan. 2024. "Information Security Evaluation of Data Centre Architecture Using COBIT 5." *Sinkron* 9(1): 466–76.

Parlika, Rizky et al. 2020. "Implementasi Akses Mysql Dan Web Server Lokal Melalui Jaringan Internet Menggunakan Ngrok." *JIKO (Jurnal Informatika dan Komputer)* 3(3): 131–36.

Permata, A A N, and E Ratnawati. 2023. "Tinjauan Kasus Cyber Phising 16 Shop Berdasarkan UU ITE Nomor 19 Tahun 2016." *UNES Law Review* 6(1): 2771–79. https://www.review-unes.com/index.php/law/article/view/1053%0Ahttps://www.review-unes.com/index.php/law/article/download/1053/823.

Rosnidar, Zulfan, and Nurasiah. 2020. "Pengaruh Penggunaan Media Pembelajaran Sejarah Infografis Pada Materi Pergerakan Nasional Terhadap Minat Belajar Sejarah Siswa Kelas XI IPS SMA Negeri 1 Darul Makmur Kabupaten Nagan Raya Dasarnya Pengarahan Siswa Oleh Guru Siswa Akan Mengalami Perubahan S." *Jurnal Imiah Mahasiswa Pendidikan Sejarah* 5: 41–53.

Syafitri, Wenni et al. 2022. "Social Engineering Attacks Prevention: A Systematic Literature Review." *IEEE Access* 10: 39325–43.

Ubaidillah, Agfar Dani Noval Kurnia, and Ruth Vanya Octaviany. 2022. "Kejahatan Cybercrime Di Era 4.0." *Seminar Nasional Ilmu Ilmu Sosial Universitas Negeri Surabaya* 2022: 776–83.

Yurita, Irma, M Kevin Ramadhan, M Candra, and Universitas Muhammadiyah Kotabumi. 2023. "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime." *Jurnal Hukum Legalita*: 144–55. https://jurnal.umko.ac.id/index.php/legalita/article/view/995.