Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-10

Analisis Keamanan Media Sosial terhadap Serangan *Phising Online* menggunakan Metode *Zphisher* dan *Social Engineering Toolkit*

Khairunnissa Zahran Ansyafa*, Muhammad Fajarudin, Muhamad Fadhil, Shelvie Nidya Neyman

Sekolah Vokasi, IPB University

Abstrak: Penelitian ini menganalisis keamanan media sosial terhadap serangan *phishing online* menggunakan metode Zphisher dan *Social Engineering Toolkit* (SET). Tujuan utama penelitian adalah mengidentifikasi teknik-teknik *phishing* yang digunakan oleh Zphisher dan SET, serta menguji apakah halaman media sosial dapat dikloning untuk mencuri data pengguna saat *login*. Selain itu, penelitian ini mengeksplorasi penggunaan email *spoofing* sebagai media untuk menyebarkan tautan *phishing*. Metode penelitian meliputi pendekatan kualitatif melalui studi pustaka dan pendekatan kuantitatif dengan eksperimen menggunakan *virtual machine* Kali Linux. Hasil penelitian menunjukkan bahwa semua platform media sosial yang diuji rentan terhadap serangan *phishing* dan email *spoofing*, membuktikan efektivitas metode yang digunakan dalam mengkloning halaman web dan mencuri data pengguna. Studi ini menekankan pentingnya meningkatkan kesadaran masyarakat tentang ancaman *phishing* dan email *spoofing* terhadap keamanan informasi di media sosial.

Kata kunci: Email *Spoofing, Phising, Zphisher, Social Engineering Toolkit*, Kali Linux

DOI: https://doi.org/10.47134/pjise.v1i4.2641
*Correspondence: Khairunnissa Zahran Ansyafa
Email: zahransyf1802ansyafa@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *This research analyzes social media security against online phishing attacks using the Zphisher method and the Social Engineering Toolkit (SET). The main aim of the research is to identify phishing techniques used by Zphisher and SET, as well as test whether social media pages can be cloned to steal user data when logging in. Additionally, this research explores the use of email spoofing as a medium for spreading phishing links. Research methods include a qualitative approach through literature study and a quantitative approach using experiments using the Kali Linux virtual machine. The results showed that all tested social media platforms were vulnerable to phishing and email spoofing attacks, proving the effectiveness of the methods used in cloning web pages and stealing user data. This study emphasizes the importance of increasing public awareness about the threat of phishing and email spoofing to information security on social media.*

Keywords: *Email Spoofing, Phishing, Zphisher, Social Engineering Toolkit, Kali Linux*

Pendahuluan

Teknologi informasi dapat mengubah ekonomi, budaya, politik, dan hukum. Namun, selain menghasilkan manfaat bagi banyak orang, perkembangan teknologi informasi juga akan memicu kejahatan baru yang dikenal sebagai kejahatan siber melalui Internet (Kharisma Putra et al., 2023). Jumlah pengguna internet yang meningkat juga menimbulkan ancaman terhadap privasi yang dapat mengancam data pribadi (Aklani et al., 2024)

Pesatnya perkembangan teknologi saat ini sangat membantu orang dalam berkomunikasi dan mengakses berbagai aplikasi online, seperti fintech, game online, belanja, kartu kredit, aplikasi perbankan, streaming video, musik, dan lainnya (Hayati & Fata, 2021).

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 (Khoirunnisaa et al., 2024)

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 (Ariani et al., 2023).

Serangan keamanan sistem informasi (*security attack*) sering terjadi (Safitri et al., 2020). *Organization of European Community Development* (OECD) mengatakan bahwa *cybercrime* mencakup semua jenis akses ilegal terhadap transmisi data. Tindakan *cybercrime* ini meningkat seiring dengan perkembangan teknologi digital, komunikasi, dan informasi (Sutabri et al., 2023). Mengingat kegiatan kejahatan dunia maya seperti *carding, hacking*, penipuan, terorisme, dan penyebaran informasi yang meresahkan, *cybercrime* merupakan fenomena yang sangat mengkhawatirkan (Gulo et al., 2021).

Cybercrime tidak jauh dari masalah sistem keamanan jaringan, karena informasi merupakan aset kunci untuk mencapai keandalan dalam implementasi keamanan jaringan (Hidayah, 2020). *Social engineering* adalah serangan dengan teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan data . Jenis serangan yang dilakukan termasuk penipuan dan pencurian data (Wahyuni et al., 2022).

Website atau situs ialah kumpulan halaman web beserta file pendukungnya yang disimpan di server web yang umumnya dapat diakses melalui Internet (Zabar & Novianto, 2015). Tautan palsu yang akan mengarahkan pengguna menuju halaman berbahaya dan berpotensi melakukan pencurian data pribadi (Firly et al., 2023).

Email *spoofing* membahayakan karena memanipulasi data pada *header* email untuk menyamar sebagai individu atau organisasi yang sah, Salah satu contohnya adalah mengirim email dengan nama pengirim seolah-olah dia adalah administrator organisasi. Pengirim email palsu menggunakan berbagai isi pesan untuk membuat korban berpikir bahwa email tersebut adalah asli (Suryana et al., 2016).

Serangan email didasarkan pada penggunaan email tingkat lanjut, karena selain digunakan untuk mengirim dan menerima pesan email juga digunakan untuk memvalidasi

informasi rahasia yang terhubung dengan berbagai akun media sosial. Serangan *phishing* adalah jenis serangan email *spoofing* yang paling terkenal karena penyerang biasanya mengambil informasi rahasia dari korban. Salah satu contoh serangan *phishing* adalah dengan menyamar sebagai email resmi dari bank (Pandove et al., 2010).

Salah satu kejahatan yang paling cepat berkembang internet ialah *phising* (Kharisma Putra et al., 2023). *Phising* merupakan salah satu jenis penipuan *cyber* yang bertujuan untuk mencuri akun korban secara ilegal (Kharisma Putra et al., 2023). *Cybercrime* dalam bentuk *phishing* ini adalah kejahatan siber yang tidak hanya melibatkan pemalsuan data pada situs web palsu yang tampaknya mirip dengan situs web aslinya (Gulo et al., 2021), tetapi juga secara ilegal untuk mendapatkan informasi pribadi atau rahasia dari korban (Sari & Sutabri, 2023). Di sisi lain, ancaman juga dapat mengakibatkan akses atau pencurian sumber daya oleh pihak yang tidak berwenang. Potensi ancaman terhadap keamanan jaringan dapat datang dari pengguna internal maupun eksternal (Sartomo & Sulistyo, 2022). Menjaga keamanan sistem informasi sangat penting untuk melindungi sistem dari setiap bahaya yang dapat membahayakan keamanan pelaku sistem dan keamanan data informasi. (Herlambang et al., 2020).

Dalam situasi lain *cyber crime* dapat ditemukan di berbagai media, seperti pesan email yang dikirimkan secara terus menerus, sehingga user akan melihat pesan secara otomatis dimana isi pesan tersebut merupakan link yang digunakan untuk melancarkan *phising* dimana link tersebut seolah-olah dibuat agar user mengikuti isi pesan tersebut yang akan dialihkan ke *website* yang menjadi media untuk melakukan eksekusi *phising* atau biasa dikenal dengan Email *Spoofing*.

Penelitian yang dilakukan oleh (Hayati & Fata, 2021) ialah memeriksa keamanan informasi media sosial dengan menggunakan setoolkit, sebuah alat untuk *phising*. Hasil penelitian menunjukkan bahwa pengkloningan URL Facebook.com akan menghasilkan halaman utama Facebook yang diakses dengan IP address pelaku *phising*. Ini menunjukkan bahwa pengujian mengkloning halaman Facebook dengan metode *phising* berhasil. Hasil penelitian menunjukkan bahwa phising dapat terjadi di semua media sosial.

Tujuan dari penelitian ini adalah untuk menguji situs media social dan melihat apakah situs tersebut dapat direplikasi sehingga terjadi pencurian data saat login. Oleh karena itu, pengujian dilakukan menggunakan settoolkit di Kali Linux.

Kali Linux adalah distribusi Linux turunan Debian yang dirancang untuk *digital forensic* dan *penetration testing*. Dari segi performa, Kali Linux telah mendapat perhatian khusus karena efisiensinya dalam menjalankan pengujian penetrasi keamanan (Luthfan et al., 2024)

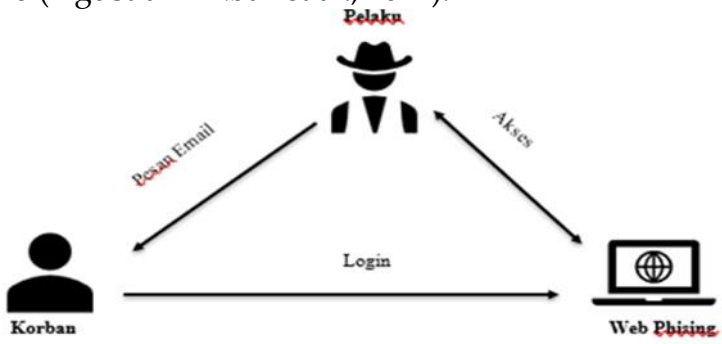
Metode

Teknik pengumpulan data yang digunakan pada penelitian ini yaitu 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 eksperimen pada sebuah virtual machine Kali Linux kemudian diimplementasikan untuk menganalisis keamanan pada website media sosial

yang tertuju seperti Instagram, Facebook, Email dan lain-lainnya. Pada virtual machine tersebut nantinya akan muncul data-data penting dari korban yang sudah mencoba mengakses *website phising* tersebut.

Terdapat 5 tahapan yang dilakukan pada proyek penelitian ini, sebagai berikut:

1. Studi literatur, melakukan tinjauan pustaka dalam memahami konsep dasar *phising* dengan metode zphisher dan SET pada Kali Linux. Tinjauan pustaka dalam penelitian ini didasarkan pada beberapa artikel, *website*, jurnal, makalah, dan sumber lain yang berkaitan dengan penelitian ini (Daila Sari et al., 2023).
2. Semua sumber yang digunakan dalam penelitian ini tercantum pada bagian "Referensi".
3. Perancangan, menyiapkan lingkungan penelitian untuk melakukan penelitian berupa menjalankan skenario (Agustian Akbar et al., 2024).



Gambar 1. Skenario Phising

4. Implementasi, dimulai dengan penyiapan alat dan lingkungan yang melibatkan instalasi Zphisher dan SET,
5. Simulasi, simulasi serangan phishing dengan membuat dan mengirimkan halaman phishing. Penyerang akan mengirimkan suatu broadcast yang memberikan arahan bagi korban untuk menelusuri *website phising*. Nantinya korban akan mencoba akses *website* tersebut, lalu penyerang akan mengumpulkan data melibatkan monitoring aktivitas di halaman phishing dan mencatat respons dari platform media sosial.

Hasil dan Pembahasan

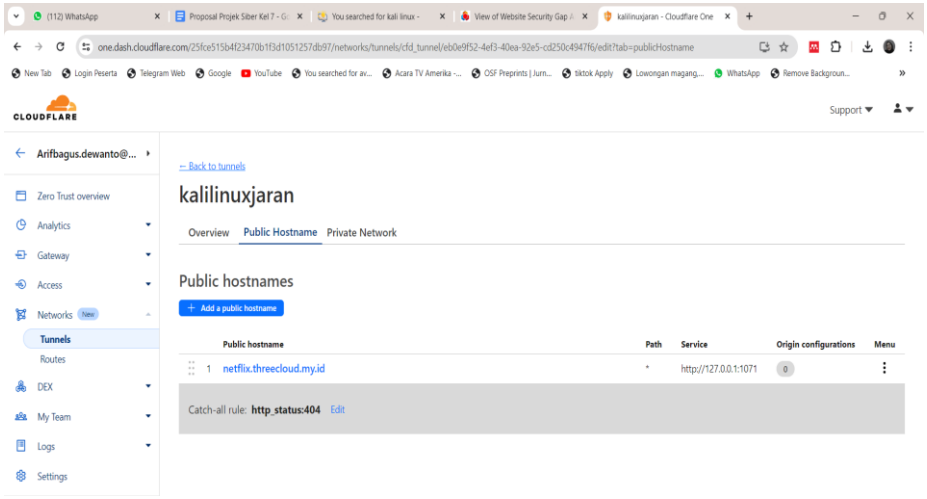
A. Phising menggunakan tools Zphisher pada Kali Linux

Zphisher merupakan salah satu tools yang dapat digunakan oleh pelaku kejahatan dunia maya yang bertujuan untuk melakukan phising terhadap website yang akan diserang, Zphisher telah menyediakan berbagai macam template yang dapat digunakan dalam melakukan phising, template yang tersedia pada Zphisher merupakan situs web yang sangat populer digunakan oleh remaja. Untuk menggunakan Zphisher disarankan untuk mengunduh versi terbarunya yang tersedia di github. Kemudian setelah memilih laman website yang akan digunakan Zphisher akan melakukan cloning website. Laman website hasil dari cloning dapat disebar luaskan ke target dengan berbagai cara salah satunya menggunakan email dengan teknik spoofing.

Gambar 2. Phising menggunakan Zphisher

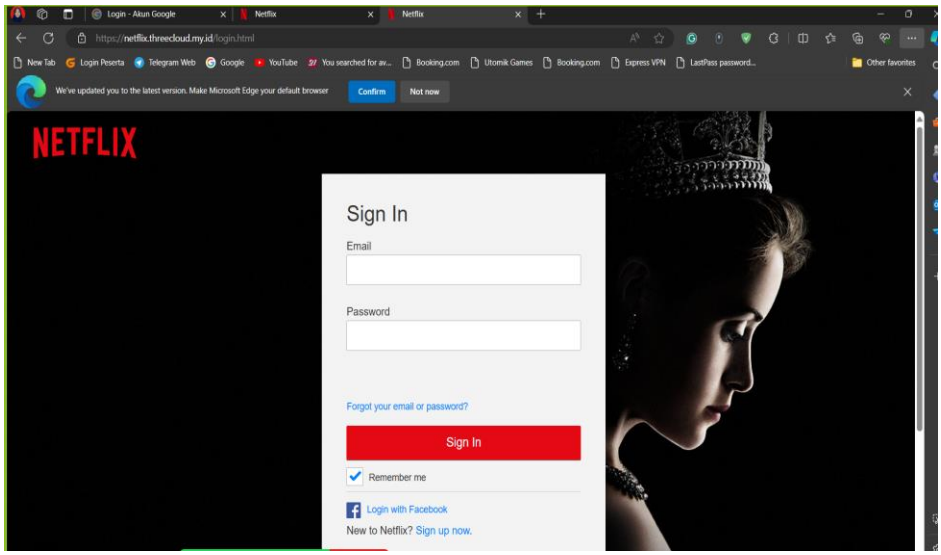
B. Akses ke Cloudflare

Cloudeflare merupakan aplikasi yang banyak digunakan sebagai media untuk melakukan distribusi domain publik dari jaringan lokal sehingga 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 cloudeflare.



Gambar 3. Konfigurasi Tunels Jaringan Local Website Phising

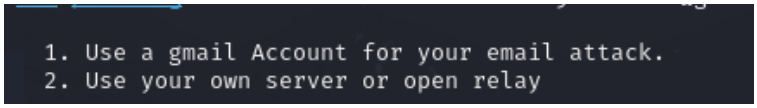
Setelah dilakukan konfigurasi Cloudeflare akan digunakan sebagai pendistribusian domain publik ke jaringan lokal pelaku kejahatan dunia maya, sehingga website yang dibuat untuk melakukan phising dapat diakses oleh korban yang dituju.



Gambar 4. Pendistribusian localhost ke domain publik menggunakan Cloudeflare

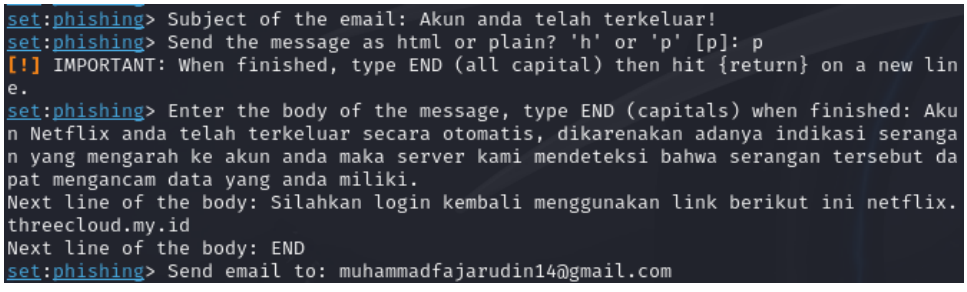
C. Pembuatan Email Spoofing

Email spoofing merupakan salah satu media untuk melakukan penyebaran tautan yang berisikan website phising yang akan diakses oleh korban. Untuk melakukan email spoofing penyerang memerlukan alamat email atau server yang dapat digunakan sebagai media serangan.



Gambar 5. Persiapan Set Toolkit

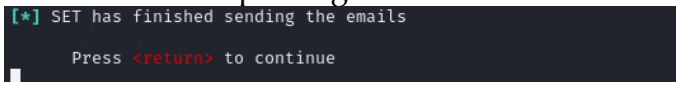
Setelah memiliki alamat email atau server penyerang diharuskan memiliki template email yang dapat menyakinkan bahwa korban merasa harus membuka link phising tersebut. Setelah itu penyerang diharuskan memiliki daftar email yang akan dijadikan korban penyerangan email spoofing.



Gambar 6. Proses Phising Email

D. Melakukan Eksekusi Penyerangan

Dalam melakukan eksekusi penyerangan phising website, hacker memiliki beberapa tahapan yaitu memastikan bahwa email spoofing telah terkirim kealamat email korban

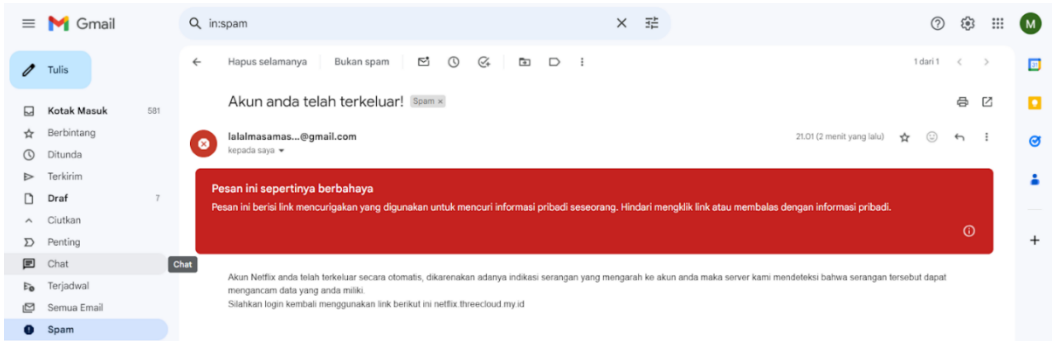


Gambar 7. Pengiriman Pesan Email Ke Alamat Email Korban

Untuk memastikan hal tersebut hacker dapat melihat pada email di tab terkirim, maka hacker akan melihat pesan email serta alamat email yang telah tertuju kepada korban.

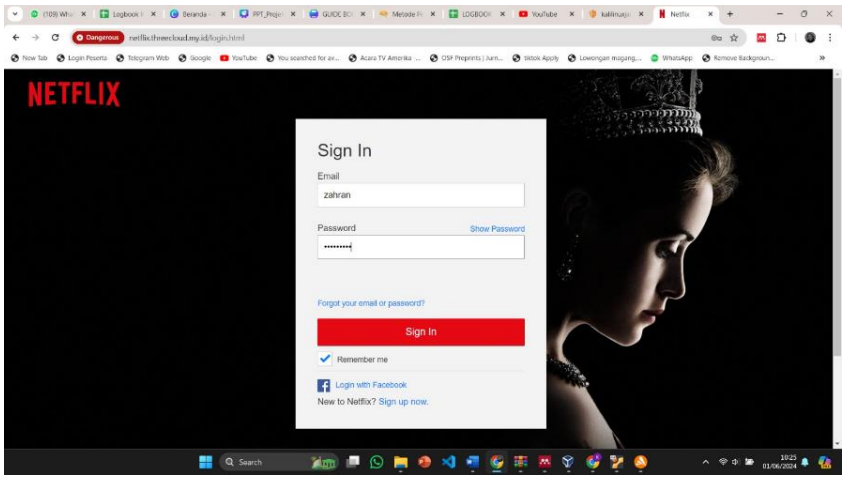
Gambar 8. Tampilan Pesan Email Telah Terkirim Ke Email Korban

Maka korban akan menerima pesan yang telah dikirimkan sehingga korban merasa link phising tersebut harus diklik.



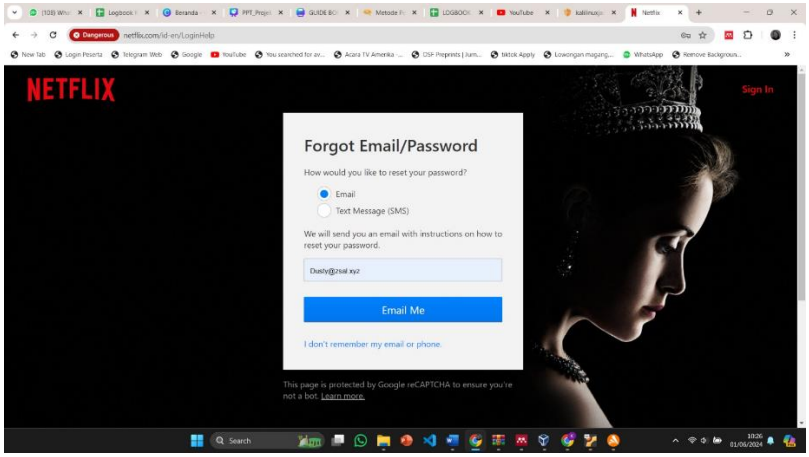
Gambar 9. Tampilan Pesan Email Spoofing Pada Korban

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.



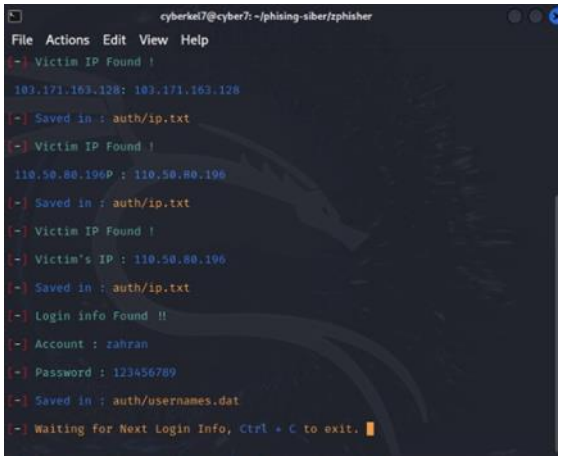
Gambar 10. Tampilan Website Netflix Phising Pada Korban

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



Gambar 11. Halaman Forgot Password

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



Gambar 12. Akun Korban Telah Didapatkan Oleh Hacker

Simpulan

Penelitian ini berhasil mengidentifikasi dan menguji teknik-teknik phishing menggunakan Zphisher dan Social Engineering Toolkit (SET) pada platform media sosial. Hasilnya menunjukkan bahwa semua media sosial yang diuji rentan terhadap serangan phishing, yang memungkinkan halaman web dikloning untuk mencuri data pengguna. Penggunaan email spoofing sebagai media untuk menyebarkan tautan phishing terbukti efektif dalam menipu pengguna agar mengakses halaman phishing. Temuan ini menggarisbawahi pentingnya meningkatkan kesadaran masyarakat tentang ancaman phishing dan email spoofing untuk menjaga keamanan informasi di media sosial. Dengan demikian, penelitian ini memberikan kontribusi penting dalam pemahaman tentang kerentanan keamanan media sosial dan perlunya tindakan pencegahan yang lebih baik.

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.

Aklani, S. A., Haeruddin, & Putri, N. (2024). IMPLEMENTASI MAIL GATEWAY SECURITY DALAM MENINGKATKAN Sistem Informasi Universitas Internasional Batam Abstraksi Development Life Cycle (NDLC), meliputi tahapan Analisis yang melibatkan identifikasi ancaman dan gateway dengan memanfaatkan layanan Aktiva. *Journal of Information System Management (JOISM)*, *5*(2).

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

Daila Sari, I., Hariyadi, D., Sahtyawan, R., & Kusumaningtyas, N. I. (2023). Analisis Tingkat Security Awareness-Personal Threat Terhadap Ancaman Phishing Dengan Metode Technology Threat Avoidance Theory (TTAT). *Teknomatika: Jurnal Informatika Dan Komputer*, *16*(2), 49–55. https://doi.org/10.30989/teknomatika.v16i2.1250

Firly, A., Egitha, H., Informatika, J. T., & Sidoarjo, U. M. (2023). *IMPLEMENTASI CLICKJACKING DALAM SERANGAN TAUTAN PALSU UNTUK EKSPLORASI MEDIA SOSIAL*. *XII*(2), 15–18.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Hayati, M., & Fata, D. (2021). Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising. *Djtechno Jurnal Teknologi Informasi*, *2*(1), 21–28. https://doi.org/10.46576/djtechno.v2i1.1252

Herlambang, P. M., Anjani, S., Wijayanto, H., & Murni, M. (2020). Cyber Security Behavior Model on Health Information System Users During Covid-19 Pandemic. *Cyber Security Dan Forensik Digital*, *3*(2), 27–33. https://doi.org/10.14421/csecurity.2020.3.2.2152

Hidayah, I. R. (2020). Representasi Social Engineering Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall). *Tibanndaru : Jurnal Ilmu Perpustakaan Dan Informasi*, *4*(1), 30. https://doi.org/10.30742/tb.v4i1.905

Kharisma Putra, I. K. O., Darmawan, I. M. A., Juliana, I. P. G., & Indriyani. (2023). Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising. *Cyber Security Dan Forensik Digital*, *5*(2), 77–82. https://doi.org/10.14421/csecurity.2022.5.2.3797

Khoirunnisaa, N., Nabila, K., Kesuma, N., Setiawan, S., Yunizar, A., & Yusuf, P. (2024). Klasifikasi Teks Ulasan Aplikasi Netflix Pada Google Play Store Menggunakan Algoritma Naive Bayes dan SVM. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, *7*(1), 64–73.

Luthfan, A., Hindami, A., Firmansyah, D. R., & Anggoman, C. R. (2024). *CESS Komparasi Kinerja CPU dan Memori dalam Proses Klasifikasi Malware Menggunakan Algoritma*

Random Forest pada Sistem Operasi Kali Linux 64-bit dan Ubuntu 64-bit Comparison of CPU and Memory Performance in Malware Classification Process Using Random Fore. *9*(1), 106–118.

Pandove, K., Jindal, A., & Kumar, R. (2010). Email Spoofing. *International Journal of Computer Applications (0975 – 8887) Volume 5– No.1, August 2010*, *5*(1), 27–30. https://doi.org/10.5120/881-1252

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(2), 21–26. https://doi.org/10.33005/jifti.v2i2.26

Sari, P., & Sutabri, T. (2023). Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. *Jurnal Digital Teknologi Informasi*, *6*(1), 29. https://doi.org/10.32502/digital.v6i1.5620

Sartomo, S., & Sulistyo, W. (2022). Model Keamanan Jaringan Menggunakan Firewall Port Blocking. *Krea-TIF: Jurnal Teknik Informatika*, *10*(1), 10–18. https://doi.org/10.32832/kreatif.v10i1.6678

Suryana, A. L., Akbar, R. El, & Widiyasono, N. (2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS). *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2), 111–117. https://doi.org/10.26418/jp.v2i2.16821

Sutabri, T., Sutabri, T., Darma, U. B., Keamanan, A., Digital, S., Dari, L., Cyber, A., Menggunakan, C., Open, M., Application, W., Project, S., Universitas, P., Insan, B., Project, S., Crime, C., Web, O., & Project, S. (2023). Analisis Keamanan Server Digital Library Dari Aktivitas Cyber Crime Menggunakan Metode Open Web Application. *Jurnal Sistem Komputer Musi Rawas*, *8*(1), 36–45.

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

Zabar, A. A., & Novianto, F. (2015). *KEAMANAN HTTP DAN HTTPS BERBASIS WEB MENGGUNAKAN SISTEM OPERASI KALI LINUX Program Studi Teknik Komputer – FTIK Universitas Komputer Indonesia Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*. *4*(2).