Journal of Internet and Software Engineering Vol: 1, No 2, 2024, Page: 1-11

Memahami Cara Kerja *Phishing* menggunakan *Tools* pada *Kali Linux*

Handika Saputra Harahap*, Allegra Alif Rahman, Indah Suraswati, Shelvie Nidya Neyman

Teknologi Rekayasa Komputer, Sekolah Vokasi, IPB University

Abstrak: Perkembangan teknologi yang pesat telah mengubah lanskap media sosial secara signifikan, khususnya di Indonesia dengan kemudahan akses internet yang semakin baik. Namun, perlu diingat bahwa keamanan tetap menjadi perhatian utama di era digital ini. *Phishing*, sebagai salah satu serangan siber yang sering terjadi, mengancam keamanan pengguna internet dengan mencuri informasi sensitif melalui trik dan situs palsu. Untuk mengatasi hal ini, pengguna perlu meningkatkan kesadaran dan pengetahuan mereka tentang tanda-tanda *phishing*. Melalui pelatihan yang tepat dan penerapan langkah-langkah keamanan teknis seperti autentikasi dua faktor, pengguna dapat melindungi informasi pribadi mereka secara lebih efektif. Dengan demikian, kesadaran dan kewaspadaan yang ditingkatkan akan membantu pengguna mengurangi risiko jatuh ke dalam jebakan *phishing* dan melindungi diri mereka dari ancaman siber yang terus berkembang. Secara keseluruhan, menggabungkan pendidikan tentang *phishing* dengan praktik keamanan teknis dapat membantu menciptakan lingkungan online yang lebih aman bagi pengguna jejaring sosial di Indonesia dan di seluruh dunia. Peningkatan kesadaran ini akan memberikan perlindungan lebih baik terhadap informasi pribadi pengguna.

Kata Kunci: Keamanan Siber, *Phishing, Kali Linux*

DOI: https://doi.org/10.47134/pjise.v1i2.2723
*Correspondence: Handika Saputra Harahap
Email: handikasaputra@apps.ipb.ac.id

Received: 01-02-2024
Accepted: 15-03-2024
Published: 30-04-2024

Abstract: A significant technological developments have changed the social media landscape significantly, especially in Indonesia with increasingly easy internet access. However, keep in mind that security remains a major concern in this digital era. Phishing, as a frequently occurring cyber attack, threatens the security of internet users by stealing sensitive information through tricks and fake sites. To combat this, users need to increase their awareness and knowledge of the signs of phishing. Through proper training and implementation of technical security measures such as two-factor authentication, users can protect their personal information more effectively. Thus, increased awareness and vigilance will help users reduce the risk of falling into phishing traps and protect themselves from ever-evolving cyber threats. Overall, combining education about phishing with technical security practices can help create a safer online environment for social network users in Indonesia and around the world. This increased awareness will provide better protection of users' personal information.

Keywords: *Cyber Security, Phishing, Kali Linux*

Pendahuluan

Perkembangan teknologi komunikasi dan informasi yang semakin canggih tidak lepas dari peran jaringan yang berperan untuk menghubungkan perangkat yang dimiliki manusia sehingga dapat bertukar data/informasi dalam hitungan sepersekian detik. Jaringan ini digunakan di berbagai perangkat, salah satunya adalah komputer, jaringan pada komputer merupakan himpunan interkoneksi antara dua komputer atau lebih yang terhubung dengan media kabel atau tanpa kabel (*wireless*) (Al Fikri, 2021). Pada satu sisi, perkembangan teknologi informasi yang demikian mengagumkan itu memang telah membawa manfaat yang luar biasa bagi kemajuan peradaban umat manusia (Adipa et al., 2023). Khususnya dalam pemanfaatan internet, masyarakat menjadi lebih mudah dan efektif dalam berkomunikasi maupun mencari informasi. Begitupun masyarakat Indonesia, 175,4 juta atau sekitar 64% penduduk Indonesia telah aktif menggunakan internet (Susilo Yuda Irawan dkk., 2021). Namun, dengan bertambahnya jumlah penduduk di Indonesia yang menggunakan internet, bertambah juga ancaman terhadap para pengguna internet tersebut. Penggunaan teknologi seperti internet harus digunakan oleh orang-orang yang dapat menggunakannya dengan baik, karena jika teknologi dimanfaatkan oleh oknum yang ingin melakukan kejahatan, maka fungsi utama adanya kemajuan teknologi akan tergantikan dengan sesuatu yang dapat merugikan orang. Banyak oknum kejahatan yang memanfaatkan kemajuan teknologi untuk menguntungkan dirinya sendiri, tetapi merugikan orang lain. Kejahatan-kejahatan tersebut dikenal dengan kejahatan siber atau *cybercrime* (Zahra Adisa & Nugroho, 2024). Topik penelitian serangan *phishing* menjadi salah satu kasus kejahatan siber yang marak terjadi di kalangan masyarakat dengan jumlah kasus di Indonesia pada kuartal dua 2023 mencapai 20.330 kasus (R. D. I. P. Sari et al., 2023). Dalam penanggulangan *cyber crime* atau kejahatan dunia maya melalui *phising*, harus menggunakan kriminologi *cyber* karena dengan menggunakan kriminologi saja tidak mampu menjawab permasalahan yang terjadi terhadap kejahatan *cyber* karena kriminologi hanya akan mampu menjawab kejahatan yang terjadi secara fisik dengan letak geografis tertentu (Ichsan, 2021). Oleh karena itu, sangat penting bagi mereka yang memiliki keahlian teknis untuk memperoleh pemahaman menyeluruh tentang mekanisme operasional teknologi. Seperti yang telah dijelaskan sebelumnya, kurangnya kesadaran pengguna memainkan peran penting dalam menjamurnya kejahatan dunia maya, khususnya dalam bidang kegiatan ilmiah, seperti *phishing* (Yurita et al., 2023).

Istilah *social engineering* mulai populer di kalangan praktisi IT, khususnya dibidang *cybersecurity*, karena memang saat memulai serangan ke suatu jaringan atau sistem yang tidak diketahui sama sekali sebelumnya, maka besar kemungkinan harus "bertanya" dan "mencuri dengar" dari orang-orang yang ada di sekitar target serangan (Ahmadian & Sabri, 2021)

Cybersecurity berasal dari dua kata yaitu *cyber* dan *security*. *Cyber* berarti dunia maya atau dunia internet dan *Security* berarti keamanan, sehingga pengertian sederhana dari *cybersecurity* adalah keamanan siber (Ramadhani & Raf'ie Pratama, n.d.). *Cyber-security* lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan

ketersediaan (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari *physical attack* maupun *cyber attack* (Ardiyanti, 2014). Sumber-sumber ancaman siber dapat berasal dari berbagai sumber, seperti intelijen asing (*foreign intelligence service*), kekecewaan (*disaffected employees*), investigasi jurnalis (*investigative journalist*), organisasi ekstremis (*extremist organization*), aktivitas para *hacker (hacktivist*), dan kelompok kejahatan terorganisir (*organized crime groups*)(Yusuf, 2022).

Cyber security atau keamanan siber merupakan tindakan untuk melindungi informasi di dunia maya dari aneka serangan. *Cyber security* makin populer berhubung makin banyaknya penggunaan komputer seperti desktop, laptop, smartphone, server, dan perangkat IoT (*internet of things*) serta penggunaan jaringan komputer seperti internet dalam kehidupan umat manusia sehari-hari (Budi et al., 2021).

Phising adalah jenis penipuan dunia maya yang bertujuan mencuri akun korban. Tentu saja, sebagian besar kejahatan dunia maya biasanya dimulai dengan *phising*, sehingga pengguna internet harus selalu waspada (Kadek Odie Kharisma Putra et al., 2022). Kata "*phishing*" yang muncul pada tahun 1996, banyak orang yang percaya bahwa kata tersebut berasal dari kata alternatif "memancing" serta "memancing Informasi". *Phising* juga dikenal dengan istilah "*Brand Spoofing*" atau "*Carding*" adalah variasi dari "memancing", idenya adalah umpan dibuang dengan harapan sebagian besar akan mengabaikan umpan tersebut dan ada juga beberapa akan tergoda untuk menggigit umpan tersebut (P. Sari & Sutabri, 2023). Modus operasi ini dapat terjadi melalui email, situs web palsu, atau pesan palsu yang dikirimkan melalui berbagai platform. Dengan memanfaatkan daya tarik atau ketertarikan korban, pelaku *phishing* menciptakan ilusi keamanan atau kepentingan pribadi untuk mengelabui mereka sehingga mereka secara tidak sengaja memberikan informasi yang berharga (Kajian et al., 2024). Skema rekayasa sosial dilakukan dengan menggunakan e-mail palsu yang mengaku berasal dari institusi bisnis yang sah dan dirancang untuk mengarahkan korban ke situs webpalsu yang mengelabui, sehingga korban membocorkan data keuangan seperti nama dan kata sandi (Efendy et al., 2019).

Linux adalah sistem operasi mirip Unix yang dulu dirancang untuk memberikan pengguna PC OS gratis atau Tingkat rendah sebanding dengan sistem Unix tradisonal dan lebih mahal (Yunianto et al., n.d.). Walaupun sangat banyak varian GNU/Linux hanya menyediakan aplikasi yang sudah ditentukan yang mungkin kurang bermanfaat oleh pengguna sehingga hal ini mengakibatkan banyak pengguna yang melakukan *remastering* untuk memenuhi kebutuhannya. *Remastering* adalah proses membuat sistem operasi baru dengan mengurangi atau menambahkan fitur-fiturnya dari distro GNU/Linux yang telah ada (Harjono, 2016)

Kali Linux adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan digunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. Kali linux dikembangkan oleh pengembang *Backtrack* sebelumnya yaitu Mati Aharoni bersama pengembang baru bernama Devon Kearns dari *Offensive Security* (Ruhiyat & Setiyadi, n.d.). Secara umum kali linux memiliki berbagai macam tools yang dapat dibagi ke dalam beberapa klasifikasi berdasarkan fungsi utamanya. Disebabkan oleh *tools* Kali Linux yang memiliki cukup banyak kategori, pengguna hanya akan mencoba

salah satu *tools* yang akan digunakan sebagai percobaan yang sesuai dengan studi kasus yang telah ditentukan. Studi kasus yang digunakan oleh pengguna adalah studi kasus mengenai *reverse engineering*, dimana pengguna akan menyelesaikan masalah dari studi kasus tersebut dengan menggunakan *tools* berbasis Kali Linux yang disediakan oleh Katoolin.(Putu et al., n.d.).

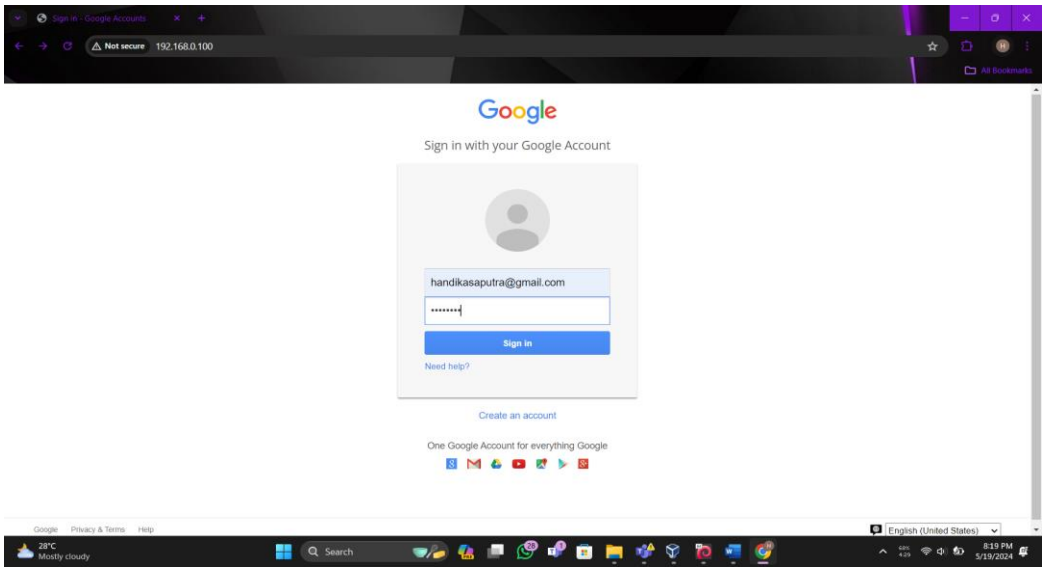
Metode

Metode penelitian yang digunakan meliputi studi literatur dan percobaan, dengan tujuan memperoleh pengetahuan yang lebih mendalam. Studi literatur dilakukan dengan mengkaji jurnal, sumber dari internet, dan referensi lainnya. Sementara itu, percobaan dilakukan secara mandiri menggunakan sistem operasi Kali Linux dan alat *Social Engineering Toolkit* (SET), serta menerapkan teknik *phishing*. Selanjutnya, mereka menyebarkan *link* atau mengirimkan pesan kepada korban untuk mengarahkan mereka ke halaman palsu tersebut. Dalam hal ini, teknik sosial rekayasa sering digunakan untuk mengelabui korban agar memasukkan informasi pribadi mereka. Setelah korban memasukkan informasi mereka, alat-alat seperti SET dapat digunakan untuk menangkap data yang dimasukkan tersebut.

Hasil penelitian menunjukkan bahwa serangan *phishing* dapat dilakukan dengan mudah dan efektif menggunakan alat-alat tersebut, menjadikannya ancaman serius bagi keamanan informasi. Selain itu, penelitian ini juga mengidentifikasi tanda-tanda umum dari situs *phishing* dan metode deteksi yang dapat digunakan oleh pengguna untuk melindungi diri mereka. Kesadaran dan pendidikan pengguna merupakan elemen kunci dalam mencegah serangan *phishing*. Pengguna harus dilatih untuk mengenali tanda-tanda *phishing*, seperti URL yang mencurigakan, kesalahan ejaan, dan permintaan informasi yang tidak biasa. Selain itu, penerapan langkah-langkah keamanan teknis, seperti autentikasi dua faktor dan penggunaan perangkat lunak keamanan yang diperbarui, dapat membantu mengurangi risiko serangan *phishing*.

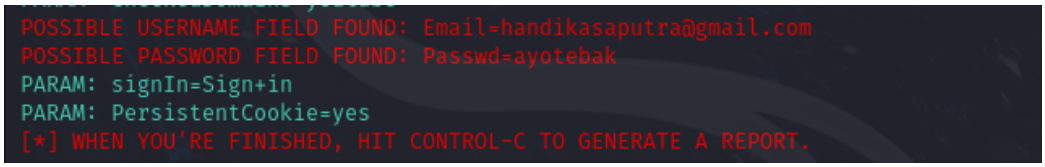
Hasil dan Pembahasan

Pada tampilan di bawah ini merupakan tampilan hasil dari *cloning* dari google.com yang menampilkan halaman web utama yang sama dengan google yang di akses menggunakan ip address. Hal tersebut dikarenakan kali linux yang kami akses menggunakan *virtualbox* maka jaringan yang didapat adalah jaringan yang terdapat pada sistem operasi utama, sehingga ip address yang didapat adalah 192.168.0.100. Ip tersebut digunakan untuk mengakses halaman *web phishing* yang sudah di *cloning*.



Gambar 1. Tampilan Login

Berikut Sebuah halaman web telah berhasil direplikasi menggunakan teknik *phising* melalui alat setoolkit. Metode yang digunakan adalah pendekatan dasar dalam *phising* yang hanya bisa diakses melalui satu jaringan tertentu. Dengan tampilan yang identik dengan halaman web aslinya, korban mudah tertipu untuk melakukan login di halaman tiruan tersebut. Setelah login, mereka akan diarahkan ke halaman web yang sesungguhnya untuk melakukan login ulang, menyelesaikan proses *phising*.



Gambar 2. Tampilan Informasi data

Pada tampilan di atas merupakan Informasi yang dimasukkan oleh korban akan otomatis tercatat di terminal pelaku. Keberhasilan replikasi halaman login Google menggunakan teknik *phising* yang sederhana telah terbukti. Namun demikian, karena pendekatan yang digunakan masih mendasar, hanya pengguna dalam satu jaringan yang bisa mengaksesnya. Walaupun URL *phising* mudah dibedakan dari yang asli, praktik ini bisa ditingkatkan dengan membuatnya menyerupai URL yang sudah terkenal, sulit dibedakan dari yang asli, dan menjangkau jaringan yang lebih luas.

Pada pengujian kali ini, kami menggunakan setoolkit di Kali Linux untuk melakukan *phising* dasar dengan mengkloning situs web resmi. Karena kami ingin menyalin situs web yang sudah ada, kami memilih opsi *site cloner* pada setoolkit. Selanjutnya, kami akan mengonfigurasi situs web yang akan digunakan. Situs web yang akan dikloning adalah halaman login pada Google.

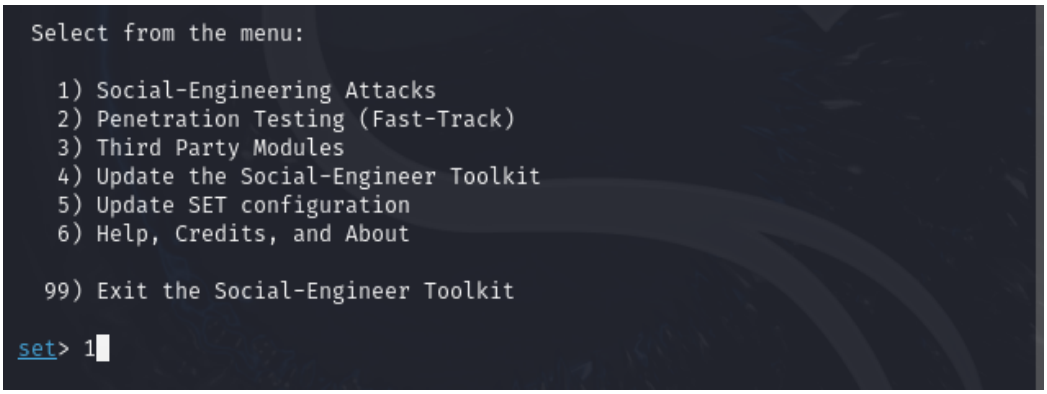
Pada gambar di bawah menunjukkan sesi terminal pada sistem operasi Kali Linux, pada prompt menunjukkan bahwa saat ini adalah "kali" dan direktori kerja adalah direktori home tersebut. Kemudian menjalankan perintah sudo su yang bertujuan untuk beralih ke root dengan hak akses superuser. Sistem kemudian meminta kata sandi untuk mengonfirmasi hak akses tersebut. Setelah kata sandi dimasukkan dan diterima, prompt berubah menjadi root, menandakan bahwa sekarang memiliki akses root. Pada prompt menunjukkan bahwa terminal sekarang berada dalam sesi root.

Gambar 3. Tampilan Sesi Root

Pada gambar di bawah menunjukkan sesi terminal di mana telah berada di mode root. Pada prompt tersebut mengketikkan perintah `setoolkit` yang digunakan untuk mengakses berbagai alat dan teknik yang tersedia di dalam toolkit.

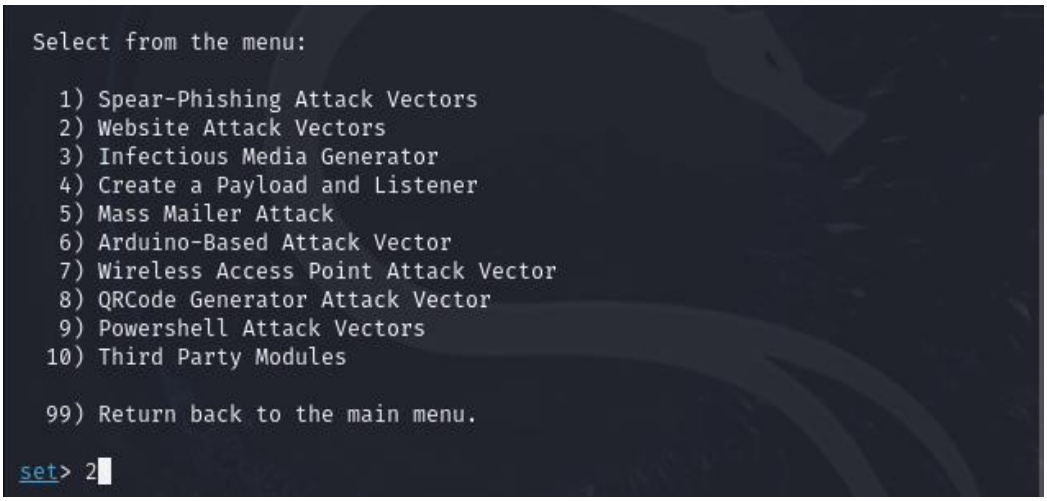
Gambar 4. Tampilan Sesi Setoolkits

Pada gambar di bawah menampilkan menu utama dari *Social-Engineer Toolkit* (SET) setelah menjalankan perintah setoolkit. Menu ini menawarkan berbagai pilihan untuk melakukan serangan rekayasa sosial dan pengujian penetrasi. Pilihan yang tersedia mencakup serangan rekayasa sosial, pengujian penetrasi cepat, integrasi modul pihak ketiga, pembaruan *toolkit*, konfigurasi SET, serta bantuan dan informasi tentang toolkit tersebut. Pada bagian bawah menu terdapat prompt set yang mengetikkan angka 1, yang mengindikasikan untuk memilih opsi "*Social-Engineering Attacks*". Perintah ini menunjukkan bahwa sedang bersiap untuk memulai serangan rekayasa sosial menggunakan SET, sebuah alat yang umum digunakan oleh peneliti keamanan dan pentester untuk menyimulasikan serangan dan menguji pertahanan keamanan jaringan.



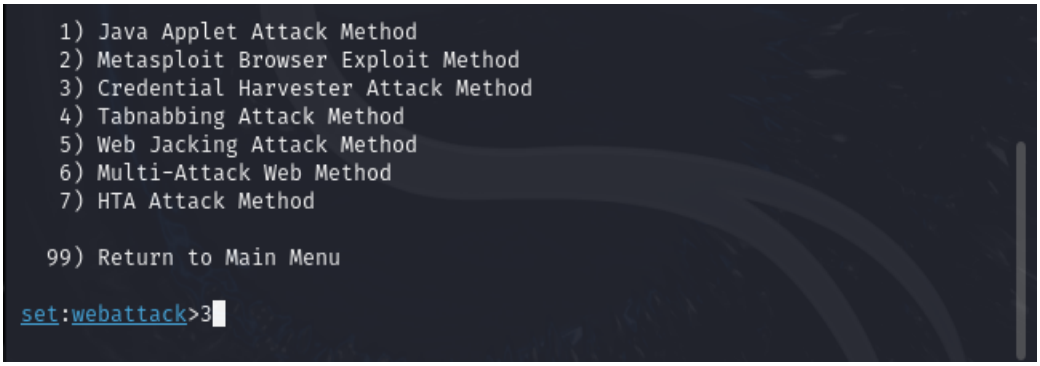
Gambar 5. Tampilan Menu Utama Toolkits

Pada gambar di bawah terdapat penjelasan Menu Utama Setoolkit yang digunakan untuk melakukan pengujian penetrasi dan simulasi serangan siber. Menu utama Setoolkit terdiri dari 10 opsi, yang memungkinkan pengguna untuk melakukan berbagai macam serangan, seperti serangan *phishing*, serangan terhadap situs web, dan serangan terhadap titik akses nirkabel.



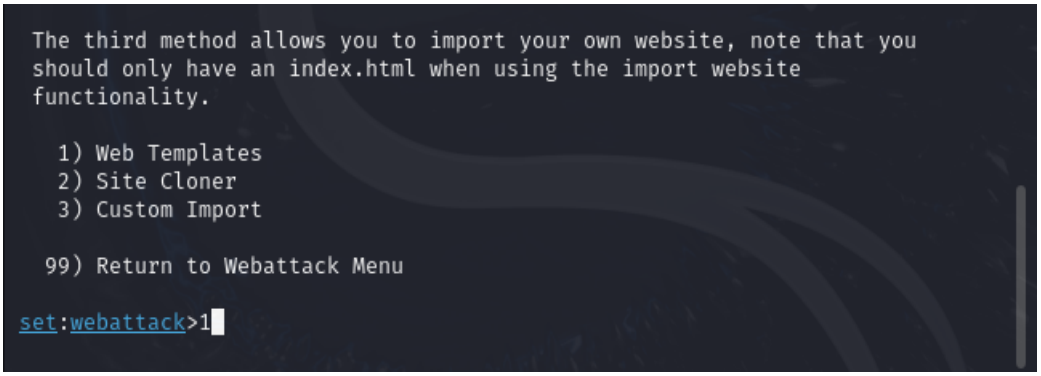
Gambar 6. Tampilan Menu Pengujian Penetrasi

Gambar di bawah menunjukkan sebuah daftar serangan yang tersedia dalam sebuah alat perangkat lunak yang digunakan untuk keamanan siber atau pengujian penetrasi. Daftar ini mencakup berbagai teknik seperti “Java Applet Attack Method”, “Metasploit Browser Exploit Method”, dan lain-lain, hingga “HTA Attack Method”. Di bagian bawah gambar, terlihat perintah yang telah di-set lalu pilih ‘3’, yang berarti memilih metode serangan “Credential Harvester Attack Method” dari daftar tersebut. Ini menarik karena memberikan wawasan tentang alat-alat dan teknik yang mungkin digunakan dalam menguji sistem untuk kerentanan.



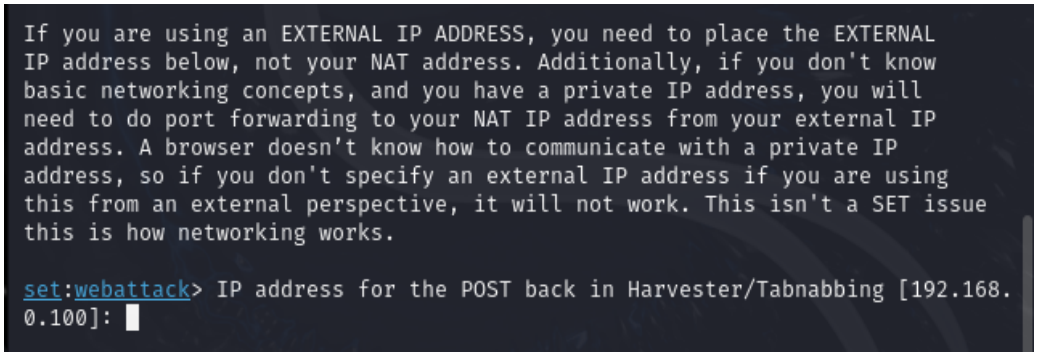
Gambar 7. Tampilan Daftar Menu Serangan

Gambar di bawah menampilkan sebuah daftar yang menjelaskan metode ketiga untuk mengimpor situs web sendiri, dengan catatan bahwa hanya file index.html yang dapat digunakan saat mengimpor situs web. Daftar tersebut mencakup tiga opsi: "Web Templates", "Site Cloner", dan "Custom Import". Di bagian bawah terdapat perintah 'set:webattack>1', yang tampaknya akan memilih opsi pertama dari menu yang disediakan. Yang artinya kita menggunakan web templates yang sudah disediakan pada tools kali linux.



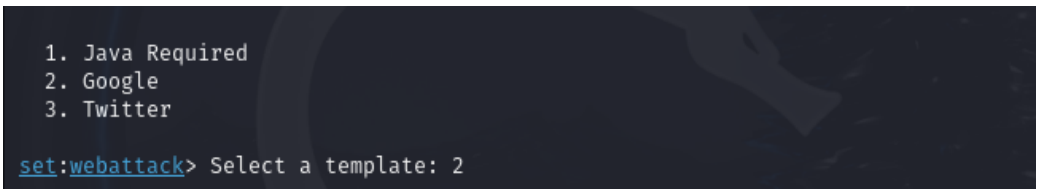
Gambar 8. Tampilan Daftar Menu Import

Pada gambar di bawah ini kita akan di berikan ip address untuk mengakses *web phishing* yang dibuat. Alamat IP 192.168.0.100 hanya dapat diakses dari dalam jaringan lokal saja, sedangkan alamat IP eksternal adalah alamat yang dapat diakses dari internet.



Gambar 9. Tampilan Akses IP

Pada gambar di bawah adalah pengujian penetrasi untuk menyimulasikan serangan rekayasa sosial. Dalam konteks kita diminta untuk memilih *template* dari beberapa opsi yang disediakan, yang akan digunakan untuk membuat halaman web palsu atau memalsukan halaman web yang sah seperti *phishing*. kemudian kita diminta untuk memilih salah satu dari *template* tersebut dengan memasukkan angka yang sesuai. Lalu kita memilih *template* nomor 2, yaitu "Google", dengan mengetik angka "2" di prompt. Ini menunjukkan bahwa untuk membuat halaman *phishing* yang menyerupai halaman login Google, yang akan digunakan untuk mengumpulkan informasi login dari target. Pilihan ini menunjukkan langkah dalam proses di mana kita menentukan jenis halaman web palsu yang ingin mereka buat untuk menjalankan serangan rekayasa sosial tertentu.



Gambar 10. Tampilan Pemilihan Templates

Simpulan

Phishing adalah praktik penipuan online di mana penyerang menciptakan situs web palsu yang meniru situs web asli dengan tujuan untuk mencuri informasi sensitif seperti kata sandi, informasi keuangan, atau data pribadi pengguna. Teknik ini seringkali digunakan dalam upaya untuk merampas identitas, mengakses akun online, atau melakukan penipuan finansial. Penting bagi pengguna internet untuk waspada terhadap tautan yang mencurigakan, memeriksa URL dengan hati-hati, dan tidak memberikan informasi pribadi atau keuangan kepada situs web yang mencurigakan. Selain itu, upaya perlindungan yang kuat, seperti menggunakan perangkat lunak keamanan yang terpercaya dan memperbarui perangkat lunak secara teratur, juga penting untuk mencegah jatuh ke dalam perangkap *web phishing*.

Berdasarkan hasil percobaan, terbukti bahwa semua media sosial rentan terhadap teknik *phishing*. Berbagai halaman dapat dengan mudah di-*cloning* untuk mengelabui pengguna, yang menyebabkan peningkatan insiden penipuan online. *Phishing* sering dilakukan dengan cara yang semakin canggih, membuat banyak pengguna tidak menyadari bahwa mereka sedang menjadi target. Oleh karena itu, diimbau kepada seluruh pengguna media sosial untuk selalu berhati-hati dan memperhatikan URL saat mengakses laman tertentu. Pengguna juga sebaiknya tidak sembarangan membagikan informasi pribadi dan selalu memverifikasi keaslian sumber sebelum memberikan data sensitif.

Selain itu, penting bagi pengguna untuk memahami tanda-tanda *phishing*, seperti URL yang mencurigakan, tata bahasa yang buruk, dan permintaan informasi pribadi yang tidak biasa. Menggunakan alat keamanan tambahan seperti autentikasi dua faktor dan perangkat lunak antivirus yang diperbarui juga dapat membantu melindungi dari serangan *phishing*. Kesadaran dan kewaspadaan pengguna merupakan kunci utama dalam mencegah terjadinya penipuan melalui media sosial. Dengan demikian, edukasi mengenai teknik-teknik *phishing* dan cara menghindarinya harus terus ditingkatkan untuk melindungi pengguna dari ancaman yang semakin berkembang ini. Upaya kolektif dari penyedia platform media sosial, pemerintah, dan pengguna sendiri diperlukan untuk menciptakan lingkungan online yang lebih aman

Daftar Pustaka

Adipa, M., Zy, A. T., Makmun Effendi, M., & Korespondensi, P. (2023). *Jurnal Restikom : Riset Teknik Informatika dan Komputer KLASIFIKASI EMAIL PHISHING MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBOR*. *5*(2), 148–157. https://restikom.nusaputra.ac.id

Ahmadian, H., & Sabri, A. (2021). TEKNIK PENYERANGAN PHISHING PADA SOCIAL ENGINEERING MENGGUNAKAN SET DAN PENCEGAHANNYA. In *Djtechno : Journal of Information Technology Research* (Vol. 2, Issue 1).

Al Fikri, K. (2021). *Keamanan Jaringan Menggunakan Switch Port Security*. *5*(2). https://doi.org/10.30743/infotekjar.v5i2.3501

Ardiyanti, H. (2014). *CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA*. http://kominfo.go.id/index.php/content/detail/3980/

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Efendy, Z., Putra, I. E., & Saputra, R. (2019). ASSET RENTAL INFORMATION SYSTEM AND WEB-BASED FACILITIES AT ANDALAS UNIVERSITY. *Jurnal Terapan Teknologi Informasi*, *2*(2), 135–146. https://doi.org/10.21460/jutei.2018.22.103

Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *Jurnal & Penelitian Teknik Informatika*, *1*(1).

Ichsan. (2021). *KAJIAN SOSIOLOGI KRIMINAL TERHADAP PENANGGULANGAN CYBERCRIME MELALUI PHISING*. https://ejournal.stisdarussalam.ac.id/index.php/jd

Kadek Odie Kharisma Putra, I., Made Adi Darmawan, I., Putu Gede Juliana, I., Kunci, K., & Crime, C. (2022). *TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING* (Vol. 5, Issue 2).

Kajian, J., Dan, H., & Kewarganegaraan, P. (2024). *Civilia* (Vol. 3, Issue 1). http://jurnal.anfa.co.id

Putu, I., Pratama, A. E., Bagus, A. A., & Wiradarma, A. (n.d.). IMPLEMENTASI KATOOLIN SEBAGAI PENETRASI TOOLS KALI LINUX PADA LINUX UBUNTU 16.04 (STUDI KASUS: REVERSE ENGINEERING FILE .APK). In *Jurnal RESISTOR* (Vol. 84, Issue 2). Online. http://jurnal.stiki-indonesia.ac.id/index.php/jurnalresistor

Ramadhani, M. R., & Raf'ie Pratama, A. (n.d.). *Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia*.

Ruhiyat, J., & Setiyadi, A. (n.d.). *SISTEM MONITORING WEBSITE DENGAN METODE ISSAF DI DINAS KOMUNIKASI dan INFORMATIKA KABUPATEN TANGERANG*.

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

Sari, R. D. I. P., Rahmah, A., Zuhroh, F., Hidayat, T. R. P., & Rakhmawati, N. A. (2023). ANALISIS BIBLIOMETRIK MENGENAI SERANGAN PHISHING PADA MEDIA SOSIAL MENGGUNAKAN VOSVIEWER. *Jurnal Ilmiah Informatika Komputer*, *28*(3), 230–240. https://doi.org/10.35760/ik.2023.v28i3.9514

Susilo Yuda Irawan, A., Heryana, N., Siti Hopipah, H., Rahma Putri, D., & Hs Ronggo Waluyo Puseurjaya Telukjambe Timur Karawang Jawa Barat, J. (2021). Identifikasi Website Phishing dengan Perbandingan Algoritma Klasifikasi. In *Syntax: Jurnal Informatika* (Vol. 10, Issue 01). www.phishtank.com

Yunianto, I., Adhiyarta, K., Bisnis, I., Bekasi, M., Budi, U., & Jakarta, L. (n.d.). *JURNAL REVIEW: PERBANDINGAN SISTEM OPERASI LINUX DENGAN SISTEM OPERASI WINDOWS*.

Yurita, I., Kevin Ramadhan, M., Candra, M., & Muhammadiyah Kotabumi, U. (2023). *PENGARUH KEMAJUAN TEKNOLOGI TERHADAP PERKEMBANGAN TINDAK PIDANA CYBERCRIME*.

Yusuf, A. L. (2022). *Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia* (Vol. 4).

Zahra Adisa, A., & Nugroho, A. A. (2024). *Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk*. *10*(1). https://doi.org/10.33506/jurnaljustisi.v10i1.xxxx