Jurnal Ilmiah
Teknologi Informasi dan Robotika

ISSN (Online): 2686-4339
Volume 6 Nomor 1, Juni 2024
Halaman: 34-43

Implementasi *Phishing Wireless* dengan Metode *Wardriving* untuk Akses *Wi-Fi*

*Ryvana Suthelie, Danang Haryo Sulaksono, Gusti Eka Yuliastuti

Institut Teknologi Adhi Tama Surabaya, Indonesia

Artikel Histori:
Disubmit: Januari 2024
Diterima: Maret 2024
Diterbitkan: Juni 2024

DOI
10.33005/jifti.v6i1.146

ABSTRAK

Wireless hacking adalah aktivitas peretasan atau eksploitasi terhadap pengguna jaringan Wi-Fi. Salah satu teknik serangan yang digunakan adalah phishing, yaitu memperoleh data pribadi dengan cara menipu korban melalui antarmuka palsu. Penelitian ini menerapkan teknik phishing menggunakan access point palsu untuk memperoleh kata sandi jaringan Wi-Fi target. Penelitian ini bertujuan untuk mengidentifikasi kelemahan sistem keamanan Wi-Fi terhadap ancaman phishing nirkabel. Proses serangan dilakukan dengan memanfaatkan perangkat lunak Wifiphisher dan metode wardriving untuk menemukan jaringan target. Tiga skenario serangan yang diuji meliputi Network Manager Connect, Firmware Upgrade Page, dan OAuth Login Page. Hasil pengujian di berbagai lokasi menunjukkan tingkat keberhasilan yang tinggi dalam merekam kredensial pengguna, dengan waktu tunggu yang bervariasi antar metode. Temuan ini menegaskan bahwa pengguna jaringan publik masih sangat rentan terhadap serangan berbasis rekayasa sosial. Penelitian ini juga memberikan kontribusi terhadap pemahaman tentang kelemahan keamanan jaringan Wi-Fi publik dan menunjukkan perlunya tindakan mitigasi, seperti autentikasi dua langkah atau deteksi akses poin palsu. Dengan memahami teknik ini, diharapkan dapat meningkatkan kesadaran dan pengembangan solusi pertahanan untuk sistem jaringan Wi-Fi publik.

Kata Kunci: Phising, WiFi, Wireless Hacking

How to Cite:
Suthelie, R., Sulaksono, D., H., Yuliastuti, G., E. (2024). Implementasi *Phishing Wireless* dengan Metode *Wardriving* untuk Akses *Wi-Fi*. *Jurnal Ilmiah Teknologi Informasi dan Robotika,* *6*(1), 34-43. https://doi.org/10.33005/jifti.v6i1.146.

***Corresponding Author:**
Email : gustiekay@itats.ac.id
Alamat : Jl. Arief Rahman Hakim No.100, Klampis Ngasem, Kec. Sukolilo, Surabaya, Jawa Timur 60117

PENDAHULUAN

Wireless hacking merupakan sebuah kegiatan seseorang yang melakukan tindakan peretasan atau eksploitasi maupun eksplorasi pengguna jaringan internet yang disediakan oleh WiFi (Susanto dkk., 2019). Tujuan dilakukan tindakan wireless hacking karena mereka ingin menyalahgunakan data pengguna dengan cara memanipulasi data maupun informasi yang dimiliki oleh pengguna jaringan internet WiFi tersebut. Wireless hacking juga memiliki beberapa metode peretasan yang biasa digunakan, salah satunya adalah metode *Wardriving*.

Wardriving merupakan kegiatan dari seseorang hacker yang bekerja untuk mendapatkan informasi dan akses terhadap suatu jaringan WiFi (Pratama, 2024). Umumnya Teknik Wardriving ini digunakan untuk mendapatkan koneksi dari jaringan internet, namun ada banyak juga yang menggunakan Teknik ini untuk disalahgunakan, seperti untuk mengeksploitasi kelemahan jaringan WiFi tersebut dam menggunakannya untuk kepentingan pribadi dari hacker (Etta dkk., 2022).

Phishing merupakan cara yang dilakukan untuk mendapatkan data seseorang dengan teknik mengelabuhi. Phishing mengincar data pribadi seperti username, password, informasi kartu kredit dan informasi rekening. Kegiatan phishing ini memang bertujuan untuk memancing seseorang memberikan informasi data pribadi tanpa disadari orang tersebut (Wibowo, 2022). Cara kerja dari phishing adalah penyerang membuat sebuah akses poin palsu yang sudah dibekali web phishing dengan nama yang sama seperti jaringan WiFi yang menjadi target, lalu menunggu pengguna masuk menggunakan akses poin palsu yang sudah dibuat untuk mendapatkan informasi dari WiFi aslinya (Nurdin dkk., 2016).

Pada penelitian sebelumnya oleh Sri Wahyuni dkk telah dijelaskan bagaimana penyerangan social engineering yang terus meningkat hingga saat ini (Wahyuni dkk., 2022). Dimana hal ini terjadi karena pelaku yang mengetahui bahwa rantai terlemah pada sebuah sistem keamanan jaringan adalah pengguna. Teknik phishing yang digunakan adalah teknik phishing email spoofing dimana teknik ini merupakan salah satu dari jenis penyerangan social engineering yang dilakukan dengan menggabungkan black eye dan stoolkit. Teknik phishing email spoofing merupakan salah satu bentuk kegiatan kriminal yang menerapkan social engineering. Email spoofing juga termasuk teknik yang sering digunakan oleh spammer ke jutaan pengguna email dengan memanipulasi target seolah-olah berasal dari institusi resmi yang dapat mengarahkan target untuk melakukan kegiatan phishing.

Pada penelitian lain yang dilakukan oleh Hendri Ahmadian dan Aulia Sabri, dijelaskan tentang penyerangan phishing pada social engineering dimana saat memulai serangan tersebut ke suatu jaringan atau sistem yang tidak diketahui sebelumnya, besar kemungkinan harus bertanya pada lingkungan sekeliling target serangan dengan menggunakan keahlian dari social engineering (Ahmadian & Sabri, 2021). Social engineering juga merupakan cara untuk menemukan kelemahan dari pengguna. Penyerangan ini dapat memanfaatkan media seperti Facebook, Email, Instagram, Twitter, Whatsapp dan beberapa aplikasi sosial media lainnya untuk mendapatkan informasi dari korban atau target (Ardy dkk., 2024). Tujuan dari penelitiannya adalah untuk menjelaskan bagaimana cara hacker melakukan penyerangan dan memanfaatkan kelemahan manusia dengan menggunakan serangan phishing untuk mendapatkan informasi pribadi. Namun, masih sedikit penelitian yang secara khusus mengevaluasi efektivitas serangan phishing berbasis akses poin palsu dengan pendekatan wardriving.

Pada penelitian ini, penulis akan melakukan sebuah teknik phishing dengan menggunakan akses poin palsu yang ditujukan kepada pengguna jaringan WiFi untuk mendapatkan password dari jaringan WiFi yang sudah dijadikan target. Tujuan dilakukannya penelitian ini untuk mengidentifikasi titik lemah sebuah sistem keamanan jaringan WiFi terhadap serangan wireless hacking yang dilancarkan terhadap pengguna jaringan WiFi. Adapun manfaat dari penelitian ini agar sistem keamanan dari jaringan WiFi dapat dikembangkan tingkat sistem keamanannya.

METODE PENELITIAN

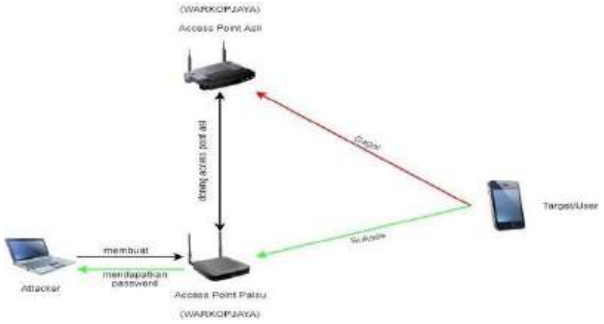
Gambaran umum pada penelitian ini mencakup bagaimana melakukan penyerangan terhadap perangkat WiFi. Penyerang akan melakukan pencarian jaringan Wi-Fi dengan kekuatan sinyal yang tinggi kemudian membuat aplikasi *phishing* pada akses poin atau membuat akses poin palsu dan berupaya untuk mendapatkan *password* atau kata sandi dari jaringan WiFi yang tersedia. Dilakukan percobaan penyerangan ini karena WiFi yang biasanya disediakan merupakan *firmware* dinamis *open-source* berbasis Linux yang bisa disesuaikan dan memiliki *package management* yang lengkap dibandingkan *firmware default* bawaan perangkat WiFi (Ye dkk., 2024). Nantinya cara kerja pengaplikasiannya yakni *phishing* tersebut akan diakses oleh *user* dan apabila *user* telah mengakses *phishing* tersebut dengan memasukkan kata sandi atau *password* dari Wi-Fi asli yang tersedia, maka penyerang akan mendapatkan kata sandi atau *password* dari jaringan Wi-Fi tersebut. Adapun rancangan sistem seperti ditunjukkan pada Gambar 2.

Penulis akan melakukan pengujian dari tingkat keamanan perangkat jaringan WiFi dengan sistem keamanan yang masih default. Adapun alur dari pengujian sistem tersebut yakni sebagai berikut:

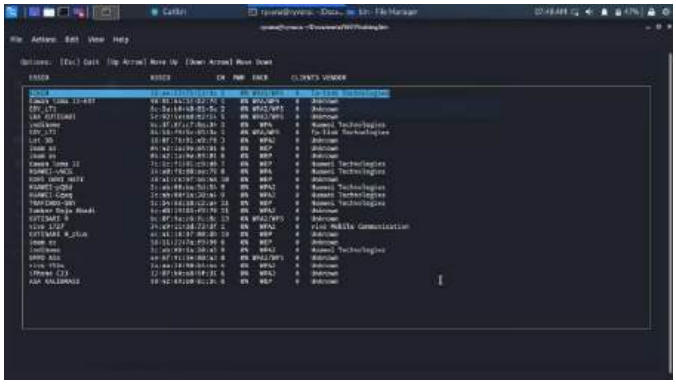
a) Penyerang melakukan pencarian perangkat Jaringan WiFi terdekat yang memiliki kekuatan sinyal kuat dengan menggunakan teknik wardriving.
b) Apabila perangkat WiFi terdekat dengan kekuatan sinyal yang kuat telah ditemukan, maka penyerang akan melakukan cloning terhadap perangkat WiFi tersebut.
c) Penyerang mengkonfigurasi program phishing yang sudah dibuat sesuai dengan perangkat WiFi yang ditemukan, kemudian melakukan scanning penyesuaian.
d) Jika scanning berhasil dilakukan, maka program tersebut berhasil dirancang sesuai dengan perangkat WiFi yang ditemukan.
e) Apabila didapati hasil scanning tidak berhasil, maka penyerang akan melakukan kembali konfigurasi program phishing yang sudah dibuat sesuai dengan perangkat WiFi yang telah ditemukan.
f) Setelah selesai melakukan cloning program, penyerang akan menunggu pengguna untuk masuk kedalam cloning perangkat WiFi yang sudah dibuat.
g) Apabila kedapatan ada pengguna yang masuk dan memasukkan password WiFi sesuai dengan perangkat WiFi asli, maka penyerang telah mendapatkan password WiFi asli dan pengguna akan dilempar ke portal WiFi yang asli. Setelah berhasil login ke WiFi yang asli, pengguna dapat mengakses jaringan tersebut tanpa tahu bahwa pengguna telah login menggunakan cloning yang sudah dibuat oleh penyerang.

HASIL DAN PEMBAHASAN

Pada pengujian *WifiPhishing* ini, terdapat 3 teknik penyerangan yang digunakan sebagai media untuk mendapatkan *password* dari *wireless fidelity* atau sering dikenal dengan Wi-Fi. Teknik penyerangan pertama yaitu *Network Manager Connect*, teknik penyerangan kedua yaitu *Firmware Upgrade Page*, teknik penyerangan ketiga yaitu *OAuth Login Page*. Pada penelitian ini, ketiga pengujian tersebut dilakukan bertujuan untuk mengetahui *password* dari pengguna yang *login* kedalam suatu jaringan Wi-Fi.



Gambar 1. Rancangan Sistem
Sumber: Data Diolah



Gambar 2. Tampilan *Network Manager Connect*
Sumber: Data Diolah

Teknik Penyerangan *Network Manager Connect*

Pertama running program *WifiPhishing* menggunakan sudo ./wifiphisher, kemudian akan muncul tampilan menu pilihan Teknik penyerangan, pilih teknik penyerangan *Network Manager Connect*. Gambar 2 merupakan tampilan *Network Manager Connect.* Setelah itu akan muncul Teknik pencarian jaringan yang menggunakan Teknik *wardriving*, lalu pilih jaringan terdekat untuk mengambil kata sandi jaringan tersebut dari pengguna yang *login.* Gambar 3 menampilkan hasil *Wardriving.* Teknik penyerangan ini bekerja dengan cara membuat tampilan layaknya "koneksi gagal" maka browser akan menampilkan jendela pengelola jaringan yang meminta password yang sebelumnya dimasukkan. Halaman ini merupakan tampilan yang biasanya muncul saat memasukkan password Wi-Fi pada umunya seperti ditunjukkan pada Gambar 5.

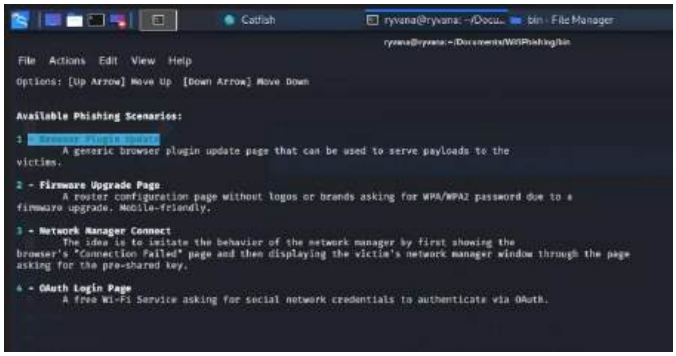
Teknik Penyerangan Firmware Upgrade Page

Pertama *running* program *WifiPhishing* menggunakan sudo ./wifiphisher, kemudian akan muncul tampilan menu pilihan Teknik penyerangan seperti ditunjukkan pada Gambar 3 dan 4, pilih teknik penyerangan *Firmware Upgrade Page*. Setelah itu akan muncul Teknik pencarian jaringan yang menggunakan Teknik *wardriving*, lalu pilih jaringan terdekat untuk mengambil kata sandi jaringan tersebut dari pengguna yang login.

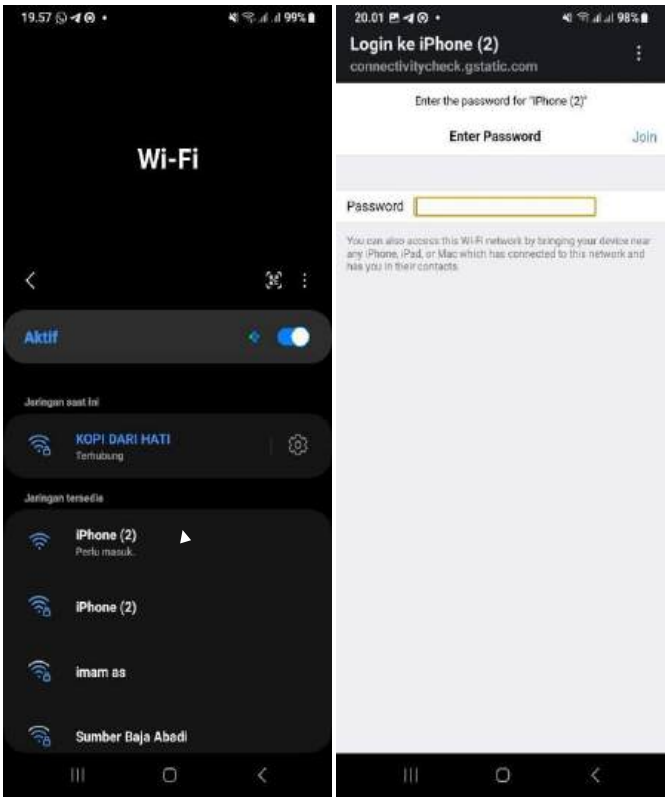
Teknik penyerangan *Firmware Upgrade Page* ini bekerja dengan cara meniru seolah-olah akses poin sedang melakukan update versi. Umumnya halaman konfigurasi *router*

tanpa logo atau merek yang meminta kata sandi dari jaringan Wi-Fi dengan sistem keamanan WPA/WPA2 karena peningkatan firmware.

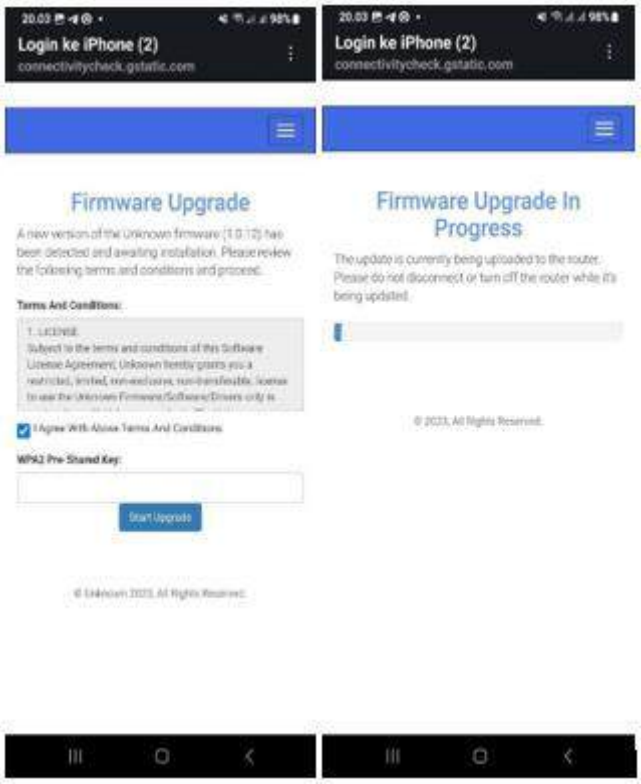
Setelah user memasukkan *password*, *password* akan terekam pada laptop penyerang, kemudian *user* akan masuk ke laman *Firmware Upgrade In Progress* namun apabila penyerang menghentikan aksi penyerangan, laman login akan tertutup otomatis dan pengguna akan masuk kembali ke akses poin asli dengan memasukkan *password* lagi.



Gambar 3. Tampilan *Wardriving*
Sumber: Data Diolah



Gambar 4. Tampilan Akses Poin Palsu dan Halaman Login
Sumber: Data Diolah



Gambar 5. Tampilan *Login Firmware Upgarde Page*
Sumber: Data Diolah

Gambar 6. Tampilan *Login OAuth Login Page*
Sumber: Data Diolah

Teknik Penyerangan OAuth Login Page

Pertama *running* program *WifiPhishing* menggunakan sudo ./wifiphisher, kemudian akan muncul tampilan menu pilihan Teknik penyerangan seperti ditunjukkan pada Gambar 3 dan 4, pilih teknik penyerangan *OAuth Login Page*. Setelah itu akan muncul teknik pencarian jaringan yang menggunakan teknik *wardriving*, lalu pilih jaringan terdekat untuk mengambil kata sandi jaringan tersebut dari pengguna yang *login*.

Pada teknik penyerangan *OAuth Login Page* ini pengguna yang *login* kedalam akses poin palsu akan diarahkan untuk masuk ke *login page* yang memiliki tampilan *login* seperti tampilan untuk *login* pada akun sosial media, seperti gmail, facebook atau twitter agar

pengguna dapat terhunung menggunakan Wi- Fi. Namun, untuk teknik penyerangan ini biasanya pengguna memiliki keraguan untuk *login*, karena takut apabila akun sosial media dari pengguna akan diambil alih dan disalahgunakan.

Setelah melakukan proses pembuatan program *phishing wireless*, kemudian melakukan pengujian dengan teknik penyerangan. Berdasarkan hal tersebut, untuk melihat suatu hasil yang sudah dikerjakan diperlukan proses pendataan secara bentuk tabel agar mengetahui nilai persentase dampak dari beberapa pengujian serangan. Untuk tahap pengujian sistem menggunakan metode *blackbox*. Metode ini memungkinkan adanya pengembangan untuk melatih seluruh fungsi pada sistem. Metode ini digunakan untuk mendemonstrasikan jalannya program dan menemukan kesalahan saat program dijalankan. Dengan menggunakan metode ini dapat dinilai apakah *input* yang diterima dan *output* yang dihasilkan sudah tepat atau belum. Adapun hasil dari pengujian sistem seperti ditunjukkan pada Lampiran 1.

Setiap teknik menghasilkan interaksi yang berbeda dari sisi pengguna. Teknik *Network Manager Connect* menyerupai kegagalan koneksi dan meminta password ulang. *Firmware Upgrade Page* menampilkan halaman pembaruan palsu dari router, sedangkan OAuth Login Page meniru login media sosial.

Lampiran 1 merangkum hasil pengujian di 10 lokasi berbeda. Tingkat keberhasilan rekaman kredensial mencapai 100% dalam setiap percobaan, namun waktu tunggu bervariasi antara 1–6 menit. Teknik OAuth cenderung berhasil di tempat dengan pengguna awam, sedangkan Firmware Upgrade Page paling efektif untuk jaringan dengan WPA2.

SIMPULAN

Berdasarkan pembahasan penelitian serta hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa teknik phishing nirkabel dengan metode wardriving terbukti efektif dalam menipu pengguna dan merekam kredensial jaringan *Wi-Fi*. *Access point* palsu yang dikonfigurasi menggunakan *Wifiphisher* juga berhasil berjalan dengan stabil tanpa gangguan berarti. Efektivitas dari setiap teknik yang digunakan ternyata bervariasi, tergantung pada lokasi serta tingkat kewaspadaan pengguna terhadap ancaman keamanan digital. Temuan ini mengindikasikan pentingnya edukasi mengenai keamanan digital, terutama bagi para pengguna jaringan publik. Untuk penelitian selanjutnya, sistem simulasi yang telah dikembangkan dapat dimanfaatkan sebagai alat edukasi maupun sarana untuk melakukan uji coba penetrasi terhadap sistem keamanan jaringan.

DAFTAR PUSTAKA

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

Ardy, L. A. F., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial. *Journal of Internet and Software Engineering, 1(4).*

Ariadi, F., Saputra, S., Putri, A. T. (2023). Sosialisasi Ancaman Dan Pencegahan Phishing Terhadap Pengguna Sosial Media Kepada Siswa/I Smk Ricardo Auto Machine. *JARI: Jurnal Pengabdian Kepada Masyarakat Republik Indonesia, 1(2)*.

Etta, V. O., Sari, A., Imoize, A. L., Shukla, P. K., & Alhassan, M. (2022). Assessment And Test-Case Study Of Wi-Fi Security Through The Wardriving Technique. *Mobile Information Systems, 2023.*

Fikri, A. W. N., et al. (2023). Analisis Keamanan Sistem Operasi Dalam Menghadapi Ancaman Phishing Dalam Layanan Online Banking. *Jurnal Ilmu Multidisiplin, 2(1),* 84–91.

Iskandar, O. (2024). Analisis Kejahatan Online Phishing Pada Masyarakat. *Leuser: Jurnal Hukum Nusantara, 1(2),* 32–36.

Nori , A., Nasution, H., & Novriando, H. (2024). Analisis Terhadap Kinerja Dan Keamanan Jaringan Nirkabel Menggunakan Teknik Wardriving Guna Mendukung Sistem Pemerintahan Berbasis Elektronik Di Kota Pontianak. *NUSANTARA JOURNAL OF MULTIDISCIPLINARY SCIENCE, 1(6),* 455–467.

Nurdin, M., Pranandi, A., Hermawan, U. D. F, Y., & Fadlapi, R. (2024). Serangan Phishing Wifi Menggunakan ESP8266: Replikasi Jaringan Untuk Penangkapan Informasi Otentikasi. *HUMANITIS: JURNAL HUMANIORA, SOSIAL DAN BISNIS*, 19(5), 1–23.

Pratama, E. (2024). Wardriving Jaringan WIFI Serta Menganalisa Qos Pada Jaringan Internet Universitas Sriwijaya Yang Tidak Terenkripsi Keamanannya. *Technologia Journal-May, 1(2),* 11–18.

Susanto, M. I., Hasad, A., & Bakri, M. A. (2019). Sistem Proteksi Jaringan WLAN Terhadap Serangan Wireless Hacking. *JREC (Journal of Electrical and Electronics), 7(1),* 25–34.

Santos, F., Pesantes, P., & Bonilla-Bedoya, S. (2021). Exploring Wardriving Potential In The Ecuadorian Amazon For Indirect Data Collection. *IOP Conference Series: Earth and Environmental Science, 690(1).*

Tuli, R. (2020). Packet Sniffing And Sniffing Detection. *International Journal of Innovations in Engineering and Technology (IJIET), 16(1),* 22–32.

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. *JNKTI: Jurnal Nasional Komputasi dan Teknologi Informasi, 5(1),* 49–55.

Ye, J., Carnavalet, X. D. C. D., Zhao, L., Zhang, M., Wu, L., Zhang, W. (2024). Exposed By Default: A Security Analysis Of Home Router Default Settings. *ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security.*

Lampiran 1. Hasil Pengujian Sistem

No.	Tempat Pengujian	Enkripsi *Password*	Hasil yang Diharapkan	Teknik Penyerangan	Pengujian dengan Teknik	Waktu Tunggu	Hasil
1	Kafe Brimob	WPA2-PSK	Pengguna *login* menggunakan *password* dari jaringan Wi-Fi kafe tersebut	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*Network Manager Connect*	3 menit 20 detik	Pengguna berhasil *login*, serta *email* dan *password* berhasil terekam
2	Jokopi Merr	WEP & WPA2	Pengguna *login* menggunakan *username wifi* dan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*OAuth Login Page*	2 menit 10 detik	Pengguna berhasil *login*, serta *email* dan *password* berhasil terekam
3	KFC Merr	WEP & WPA2	Pengguna *login* menggunakan *email* dan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*OAuth Login Page*	3 menit 2 detik	Pengguna berhasil *login*, serta *email* dan *password* berhasil terekam
4	Mie Mapan Rungkut	WPA2-PSK	Pengguna *login* menggunakan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*Network Manager Connect*	1 menit 18 detik	Pengguna berhasil *login*, serta *password* berhasil terekam
5	Warkop Bening	WPA2-PSK	Pengguna *login* menggunakan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*Firmware Upgrade Page*	4 menit 2 detik	Pengguna berhasil *login*, serta *password* berhasil terekam
6	Setunggal Dulur Kopi (STK)	WPA2-PSK	Pengguna *login* menggunakan *password*	- *Network Manager Connect*	*Firmware Upgrade Page*	5 menit 8 detik	Pengguna berhasil *login*, serta *password*

No.	Tempat Pengujian	Enkripsi *Password*	Hasil yang Diharapkan	Teknik Penyerangan	Pengujian dengan Teknik	Waktu Tunggu	Hasil
				- *Firmware Upgrade Page* - *Oauth Login Page*			berhasil terekam
7	Starbucks Merr	WEP & WPA2	Pengguna *login* menggunakan *email* dan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*OAuth Login Page*	6 menit 13 detik	Pengguna berhasil *login*, serta *email* dan *password* berhasil terekam
8	Excelso Merr	WPA2-PSK	Pengguna *login* menggunakan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*Network Manager Connect*	1 menit 32 detik	Pengguna berhasil *login*, serta *password* berhasil terekam
9	Kopi Kenangan Semolo	WEP & WPA2	Pengguna *login* menggunakan *email* dan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*OAuth Login Page*	4 menit 50 detik	Pengguna berhasil *login*, serta *email* dan *password* berhasil terekam
10	Wifi.id	WEP & WPA2	Pengguna *login* menggunakan *email* dan *password*	- *Network Manager Connect* - *Firmware Upgrade Page* - *Oauth Login Page*	*OAuth Login Page*	3 menit 49 detik	Pengguna berhasil *login*, serta *email* dan *password* berhasil terekam

Sumber: Data Diolah