Analisis Kuantitatif Eksploitasi Akun Google Pasca Phishing Berbasis Konsistensi Jaringan

Muhammad Syahrul Haq [a,1,*], Heribertus Yulianton [a,2]

[a] Universitas Stikubank, Jl. Kendeng V Bendan Ngisor, Semarang 50233, Indonesia
[1] muhammadsyahrul0038@mhs.unisbank.ac.id *; [2] heri@edu.unisbank.ac.id;
* Korespondensi penulis

Submission:15/12/2025, Revision: 19/12/2025, Accepted : 22/12/2025

Abstract

Phishing attacks experienced a significant increase during the COVID-19 pandemic, with over 160,000 phishing domains identified quarterly in 2020. This research analyzes login success using phishing-derived data through residential proxies to identify critical factors affecting attack effectiveness against Google authentication systems. Quantitative methodology with controlled experiments utilized 150 Gmail accounts created specifically for this research, with a maximum of 15 login attempts per account. Results demonstrate a 90.7% success rate (136 of 150 cases), with three dominant factors: IP address accuracy (100% match = 97.8% success rate), tier-1 Malaysia ISP/ASN matching (AS4818 DiGi 92.3%, AS9534 Maxis 91.9%, AS4788 TM 90.3%), and geographic location consistency (Kuala Lumpur 59.3% with 91% success rate). Critical findings reveal systemic vulnerabilities in Google's 7-day old password validity policy, creating a window of vulnerability where 22.1% of attacks succeeded on days 3-6 post-password change. This research contributes to cybersecurity literature by providing a quantitative framework for measuring residential proxy effectiveness in post-phishing exploitation and recommending mandatory 2FA implementation and reduction of old password validity period to maximum 48 hours.

Keywords: authentication, ASN, Gmail security, phishing, residential proxy, window of vulnerability

Abstrak

Serangan *phishing* mengalami peningkatan signifikan selama pandemi COVID-19, dengan lebih dari 160.000 domain *phishing* yang teridentifikasi setiap triwulan pada tahun 2020. Penelitian ini bertujuan untuk menganalisis faktor-faktor kritis yang memengaruhi keberhasilan log masuk (*login*) menggunakan data hasil *phishing* melalui *residential proxy* terhadap sistem autentikasi Google. Metode penelitian menggunakan pendekatan kuantitatif dengan eksperimen terkontrol terhadap 150 akun Gmail yang dibuat khusus untuk penelitian, dengan maksimal 15 percobaan log masuk per akun. Data dikumpulkan melalui simulasi serangan menggunakan layanan *residential proxy* DataImpulse dengan variasi parameter lokasi geografis, ASN/ISP, dan akurasi alamat IP. Hasil penelitian menunjukkan tingkat keberhasilan mencapai 90,7% (136 dari 150 kasus) dengan tiga faktor dominan: akurasi alamat IP (kecocokan 100% menghasilkan tingkat keberhasilan 97,8%), kesesuaian *Tier-1* ISP/ASN Malaysia (AS4818 DiGi 92,3%, AS9534 Maxis 91,9%, AS4788 TM 90,3%), dan konsistensi lokasi geografis (Kuala Lumpur 59,3% dengan tingkat keberhasilan 91%).Temuan kritis mengungkap kerentanan sistemik pada kebijakan validitas kata sandi (*password*) lama Google selama 7 hari, yang menciptakan celah keamanan di mana 22,1% serangan berhasil dilakukan pada hari ke-3 hingga ke-6 pasca-perubahan kata sandi. Penelitian ini memberikan kontribusi berupa kerangka kerja kuantitatif untuk mengukur efektivitas *residential proxy* dalam eksploitasi pasca-*phishing*, serta merekomendasikan implementasi wajib autentikasi dua faktor (2FA) dan pengurangan periode validitas kata sandi lama menjadi maksimal 48 jam guna meningkatkan keamanan akun digital.

Kata kunci: autentikasi, ASN, celah keamanan, phishing, proxy perumahan, keamanan Gmail

1. Pendahuluan

Kemajuan teknologi informasi yang pesat dalam beberapa tahun terakhir, terutama selama jangka waktu dari 2019 hingga 2020, telah memberikan pengaruh besar pada proliferasi layanan digital di Indonesia. Sesuai statistik yang diberikan oleh Asosiasi Penyedia Layanan Internet Indonesia (APJII), proporsi pengguna internet di Indonesia naik menjadi 73,7% pada tahun 2020, yang setara dengan sekitar 196,7 juta individu. Eskalasi ini, yang dipicu oleh pandemi COVID-19, telah memaksa individu untuk mengalihkan kegiatan mereka, termasuk pekerjaan, pendidikan, dan perdagangan, ke platform digital. Sementara fenomena ini menghasilkan kemajuan yang menguntungkan di bidang digitalisasi, secara bersamaan menghadirkan peluang besar untuk ancaman cyber, terutama serangan phishing[1]. Serangan phishing, yang bertujuan untuk memperoleh informasi sensitif seperti kredensial login melalui taktik menipu, telah menyaksikan peningkatan yang nyata selama pandemi. Metodologi serangan yang semakin canggih, termasuk spoofing dan penyebaran jaringan pribadi virtual (VPN), menghadirkan tantangan signifikan bagi kerangka kerja keamanan tradisional dalam hal kemanjuran deteksi. Sebuah laporan tahunan yang disebarluaskan oleh Anti-Phishing Working Group (APWG) mengungkapkan bahwa lebih dari 160.000 domain phishing diidentifikasi setiap triwulanan pada tahun 2020. Di Indonesia, Badan Siber dan Kata Sandi Negara (BSSN) juga mengamati peningkatan frekuensi laporan mengenai insiden phishing, terutama yang menargetkan akun penting seperti email dan profil media sosial[2].

Fenomena ini menggambarkan transformasi substansial; Namun, masih ada kekurangan penting dalam penyelidikan ilmiah yang menyelidiki secara komprehensif komponen login yang berhasil yang muncul dari data phishing, terutama yang menggabungkan pemanfaatan residential proxy[3]. Sebagian besar literatur yang masih ada terutama berkonsentrasi pada metodologi dan teknik yang berkaitan dengan deteksi dini serangan phishing, sedangkan sejumlah penelitian terbatas terlibat dalam pemeriksaan contoh login yang berhasil yang terjadi setelah penggunaan data yang diperoleh dari insiden phishing, terutama dalam kerangka informasi seperti alamat Protokol Internet (IP), data terkait email, dan lokasi geografis korban, di antara faktor-faktor lainnya[4]. Untuk mengurangi kerentanan ini, platform digital termasuk Google, Facebook, dan TikTok telah menggunakan berbagai langkah keamanan tambahan, salah satunya mencakup verifikasi identitas pengguna melalui mekanisme seperti "*Verify It's You*". Prosedur ini dirancang untuk memastikan bahwa individu yang mencoba mendapatkan akses ke akun memang pengguna yang berwenang. Namun demikian, pertanyaan yang muncul adalah apakah proses verifikasi identitas cukup untuk melindungi akun dari serangan phishing. Penelitian ini berkonsentrasi pada penilaian kemanjuran mekanisme verifikasi dalam menggagalkan upaya login yang berhasil dilakukan oleh pelaku phishing, serta menentukan apakah ada kerentanan yang mungkin dieksploitasi oleh penyerang[5].

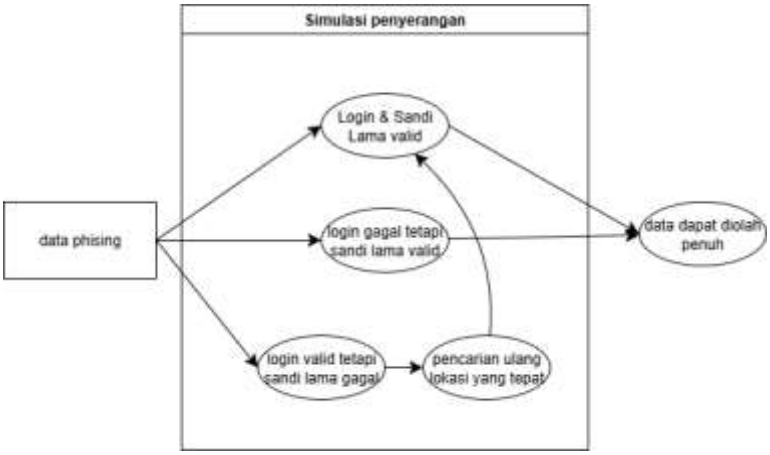
Menyoroti fakta bahwa meskipun sistem verifikasi identitas digunakan, platform seperti Google masih memberikan celah dalam pengamanan akun. Salah satu contohnya adalah kebijakan penggantian password, di mana jika pengguna mengganti password dalam kurun waktu 7 hari, akun masih berpotensi rentan terhadap serangan *phishing*[6]. Hal ini menimbulkan pertanyaan apakah penggunaan metode verifikasi identitas saja sudah cukup, ataukah tambahan langkah-langkah pengamanan, seperti autentikasi dua faktor (2FA), juga diperlukan untuk meminimalkan risiko serangan. Pendekatan kuantitatif dengan metode eksperimen langsung ini memungkinkan pemahaman yang lebih mendalam mengenai dinamika yang terjadi setelah serangan *phishing*. Dengan menggunakan data yang diperoleh dari serangan *phishing* yang melibatkan proxy untuk melakukan aksi penyerangan[7].Penelitian ini bertujuan untuk mengeksplorasi data hasil *phishing* melalui pendekatan kuantitatif. Pendekatan kuantitatif dengan metode eksperimen langsung memfasilitasi pemahaman yang lebih mendalam tentang dinamika yang terjadi setelah serangan *phishing*. Dengan memanfaatkan data yang diperoleh dari insiden phishing yang menggabungkan residential proxy sebagai perantara bagi pelaku, penelitian ini akan meneliti elemen-elemen yang berkontribusi pada keberhasilan *login*, mencakup dampak variabel seperti alamat IP, lokasi geografis, dan kategori perangkat yang digunakan oleh korban[8]. Studi ini mengantisipasi hasil yang dapat menawarkan wawasan baru tentang implikasi serangan phishing dalam lingkungan digital modern, terutama mengenai proses di mana data yang dipanen melalui phishing dapat dimanipulasi oleh penjahat untuk mengakses akun pribadi, terutama menekankan akun Google[9]. Pada tingkat teoretis, penelitian ini memiliki kapasitas untuk menambah kumpulan literatur yang ada mengenai faktor-faktor penentu yang mempengaruhi kemanjuran serangan *phishing*, selain dampaknya pada kerangka keamanan digital. Dari perspektif praktis, temuan penelitian ini dapat berfungsi sebagai dasar untuk mengembangkan strategi deteksi dan mitigasi yang lebih manjur yang bertujuan untuk menggagalkan sifat serangan *phishing* yang semakin canggih dan sulit dipahami.

2. Metode Penelitian

Informasi Login	
Email/Nomor	bashirahnur97@gmail.com
Password	si tinggi
Login	Google
Informasi Device	
Platform	Android
Os	12
Browser	AppName Mobile
Informasi Korban	
Negara	Malaysia
Wilayah	Kuala Lumpur
Kota	Kuala Lumpur
Latitude	3.2038
Longitude	101.7189
ISP	TM TECHNOLOGY SERVICES SDN BHD
Zona Waktu	Asia/Kuala_Lumpur
IP Address	180.75.245.16

Gambar 1. Contoh data

Penelitian ini menggunakan metodologi kuantitatif yang menggunakan teknik eksperimental langsung untuk mengevaluasi kemanjuran login setelah insiden phishing melalui *proxy residential* yang disediakan oleh layanan DataImpulse. Dataset utama terdiri dari 150 akun Gmail yang dibuat secara khusus untuk tujuan penelitian ini dalam lingkungan terkontrol, berisi data simulasi sensitif (termasuk email, kata sandi, alamat IP, lokasi geografis, Penyedia Layanan Internet, dan jenis perangkat) untuk mensimulasikan upaya login, dibatasi hingga maksimum 15 upaya per akun untuk menyelaraskan dengan ambang deteksi sistem keamanan. Temuan menunjukkan bahwa keberhasilan upaya login secara signifikan dipengaruhi oleh integritas tiga komponen penting: keakuratan alamat IP, konsistensi wilayah geografis, dan kesesuaian ASN/ISP, di mana kombinasi optimal dari ketiga elemen ini menghasilkan tingkat keberhasilan yang tinggi, bahkan untuk akun yang salah dalam identifikasi lokasi[10].



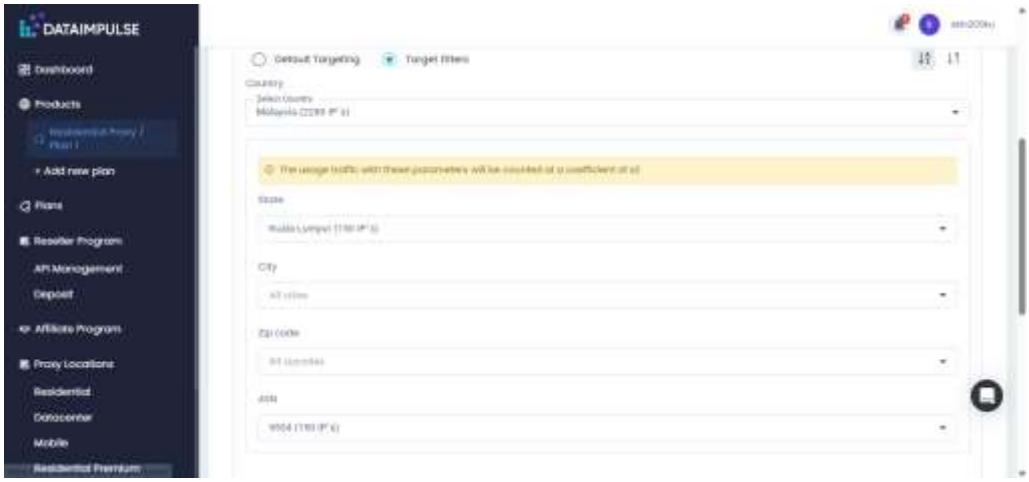
Gambar 2. Alur kerja Penelitian

Gambar 2 merupakan proses simulasi penyerangan dalam penelitian ini mengikuti alur kerja sistematis yang dirancang untuk menguji berbagai skenario eksploitasi. mengilustrasikan alur logis simulasi ini secara komprehensif. Diagram alir ini menjadi pedoman operasional selama eksperimen, memastikan semua skenario diuji secara konsisten dan data dari setiap cabang proses dapat dikumpulkan untuk dianalisis. Berikut adalah penjelasan detail untuk setiap tahap simulasi yang dilakukan:

1. *Login* dengan kata sandi lama yang sudah tidak valid tetap dapat berhasil, menunjukkan penyerang bisa memperoleh akses sementara meskipun tidak dapat mengganti kata sandi. Akses ini terbatas namun dapat berkembang menjadi akses penuh melalui beberapa percobaan tambahan.
2. *Login* dengan kata sandi lama yang masih valid memungkinkan penyerang memperoleh akses penuh, termasuk mengganti kata sandi dan mengelola akun.
3. *Login* gagal meskipun kata sandi lama masih berlaku hingga 7 hari setelah diganti. Dalam periode tersebut.
4. Implementasi dimulai dengan menyiapkan alat dan lingkungan, termasuk pemasangan super proxy pada perangkat Android sebagai penghubung ke *proxy residential* Dataimpulse.
5. Simulasi dilakukan melalui aplikasi Gmail pada perangkat Android dalam *controlled environment*, mencakup seluruh skenario serangan dari tahap pertama hingga ketiga. Data hasil simulasi dianalisis untuk menilai potensi kerentanan dan dampaknya, memberikan wawasan penting dalam upaya mitigasi ancaman siber pada platform komunikasi digital.

3. Hasil dan Pembahasan

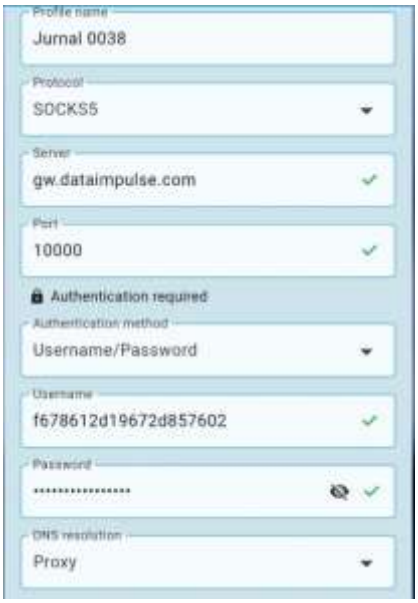
3.1 Penggunaan Residential Proxy untuk keberhasilan penyerangan



Gambar 3. Fitur Residential Proxy Dataimpulse

Gambar 3 merupakan fitur *Target Filters* pada layanan DataImpulse *Residential Proxy* digunakan untuk menyaring IP berdasarkan parameter geografis dan teknis seperti negara, provinsi, kota, kode pos, dan ASN (*Autonomous System Number*). Dalam penelitian ini, pemilihan lokasi proxy secara spesifik seperti memilih negara Malaysia, provinsi Kuala Lumpur, dan ASN 9534 bertujuan untuk menyamakan karakteristik IP dengan data asli korban *phishing* guna meningkatkan peluang keberhasilan *login*. Pemanfaatan filter ini memungkinkan percobaan login dilakukan seolah-olah berasal dari lokasi dan jaringan yang serupa dengan korban, sehingga meminimalkan deteksi oleh sistem keamanan. Namun, penggunaan parameter target yang lebih sempit seperti ini dikenakan koefisien konsumsi sebesar dua kali lipat (x2), karena keterbatasan dan eksklusivitas sumber daya IP yang digunakan[11].

3.2. Integrasi Residential Proxy menggunakan Super Proxy



Gambar 4. Integrasi Super proxy dengan Residential Proxy

Gambar 4 menunjukkan konfigurasi proxy pada perangkat *mobile* peneliti untuk mengaktifkan layanan Residential Proxy dari DataImpulse menggunakan protokol SOCKS5. Pengaturan mencakup: *Profile Name*, protokol SOCKS5, server gw.dataimpulse.com, serta port 10000 dengan rentang port antara 823 hingga 30000. Autentikasi menggunakan *username* dan *password* dari DataImpulse, serta resolusi DNS melalui proxy juga diaktifkan guna menjamin keamanan dan pembatasan akses. Penggunaan konfigurasi ini selaras dengan praktik yang digunakan dalam penelitian konfigurasi keamanan jaringan berbasis proxy [12].

3.3 Simulasi Penyerangan

3.3.1 Melakukan pencarian lokasi sesuai data

Negara	Malaysia
Wilayah	Kuala Lumpur
Kota	Kuala Lumpur
Latitude	3.1831
Longitude	101.6706
ISP	DiGi Telecommunications Sdn Bhd., Digi Internet Exchange
Zona Waktu	Asia/Kuala_Lumpur
IP Address	115.164.210.64

Gambar 5. Gambaran Informasi

Penelitian ini menunjukkan bahwa penggunaan *residential proxy* untuk menyamakan lokasi IP dengan data korban phishing tidak selalu menghasilkan akurasi lokasi yang konsisten. Sebagai contoh pada gambar 5, alamat IP terdeteksi berada di Kuala Lumpur dalam data utama, namun diidentifikasi sebagai wilayah Tampoi, Johor oleh layanan IP *tracking* lain. Ketidaksesuaian ini memengaruhi keberhasilan *login*, di mana sistem dapat mengizinkan akses awal tetapi menolak validasi lanjutan, seperti perubahan kata sandi, apabila terdapat perbedaan lokasi, ISP, atau ASN. Kondisi ini menjelaskan keberhasilan login awal dengan status kata sandi lama yang tidak lagi valid, yang menghambat akses penuh terhadap akun target[13]. Dalam konteks keamanan sistem *login*, perbedaan kecil dalam parameter jaringan dapat memicu sistem untuk menolak aktivitas *login* meskipun kredensial valid digunakan[14].

3.3.2 Perubahan IP setelah penggunaan Proxy

Gambar 6. Simulasi perubahan IP

Studi ini berdasarkan gambaran 6 modifikasi dalam perutean jaringan yang didasarkan pada informasi Nomor Sistem Otonom (ASN) dan rentang alamat IP yang dipicu oleh penyebaran *proxy* perumahan yang dikonfigurasi melalui dua pengaturan *port* yang berbeda, khususnya port 18000 dan 12000. Awalnya, koneksi berasal dari ASN AS4761 (INDOSAT) dengan kisaran alamat IP 114.10.6.0/23, yang mewakili jaringan lokal di Indonesia. Setelah aktivasi proxy menggunakan port 18000, lalu lintas data dialihkan ke ASN AS4818 Telekomunikasi DiGi yang terletak di Malaysia, ditandai dengan rentang alamat IP 182.62.0.0/15. Selain itu, ketika port 12000 digunakan, sistem sekali lagi mendokumentasikan perubahan alamat IP sambil tetap dalam ASN yang sama, yang sesuai dengan kisaran 115.164.0.0/17. Perubahan tersebut sangat penting dalam arsitektur kerangka kerja keamanan jaringan, karena kesesuaian konfigurasi port secara signifikan mempengaruhi kemanjuran prosedur simulasi serangan. Hal ini menjadi semakin penting dalam konteks *port scanning*, yang membutuhkan penyesuaian *port* sesuai dengan kondisi serta lokasi data pengujian, Menunjukkan bahwa *port scanning* merupakan teknik utama dalam pengujian efektivitas *firewall* dan sistem deteksi intrusi (IDS) pada jaringan berskala kecil dan menengah[15].

3.3.3 Melakukan *login*

Gambar 7. Verifikasi Diri Anda dalam kasus *login*

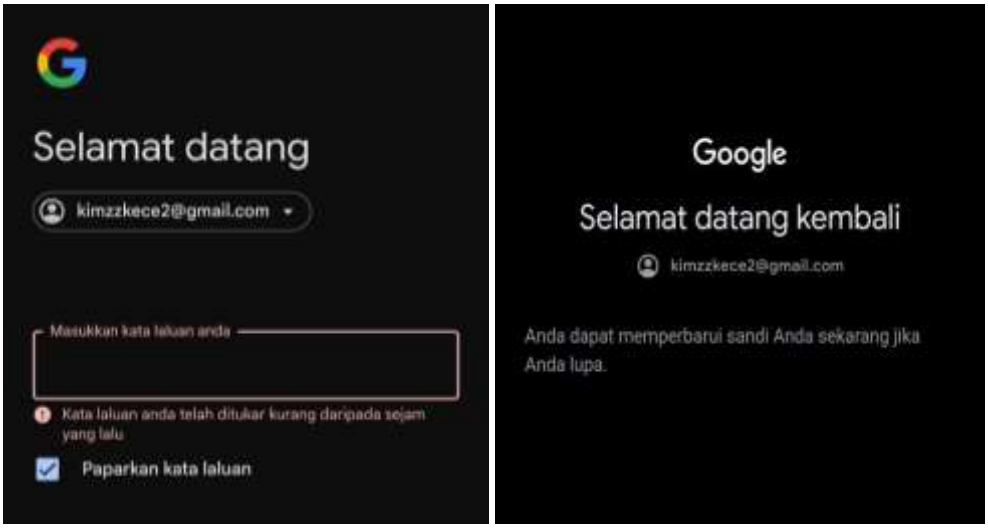
Gambar pertama ada gambar 7 pmenunjukkan skenario pengujian *login* secara langsung pada aplikasi Gmail tanpa menggunakan koneksi proxy. Sebaliknya, gambar kedua menggambarkan kondisi saat pengguna berhasil masuk ke akun Gmail hasil serangan *phishing*. Dalam tahap ini, peneliti hanya perlu menetapkan lokasi berdasarkan data yang diperoleh dari proses phishing. Apabila terjadi kesalahan atau kegagalan saat proses *login*, peneliti dapat melakukan penyesuaian dengan mengganti port yang digunakan atau mengidentifikasi ulang lokasi melalui alamat IP yang telah terekam dalam data tersebut.

3.3.4 Kasus setelah berhasil *login*

Gambar 8. Contoh mengubah kata sandi

Setelah peneliti berhasil melakukan *login* ke akun Gmail, terdapat dua kemungkinan skenario yang dapat terjadi. Pada gambar 8 kasus pertama, peneliti dapat langsung mengubah kata sandi, yang menunjukkan bahwa proses *login* berhasil secara penuh dan seluruh data dalam akun dapat diakses tanpa hambatan. Sementara itu, pada kasus kedua, sistem menampilkan fitur keamanan berupa verifikasi identitas tambahan. Kondisi ini tidak serta-merta menunjukkan kegagalan akses, melainkan menandakan adanya ketidaksesuaian kecil, seperti lokasi *login* atau konfigurasi port. Peneliti dapat mengatasi hal ini dengan menyesuaikan wilayah atau mengganti port, kemudian melakukan *login* ulang. Cukup dilakukan koreksi pada salah satu dari dua parameter tersebut untuk memperoleh kembali akses penuh ke akun.

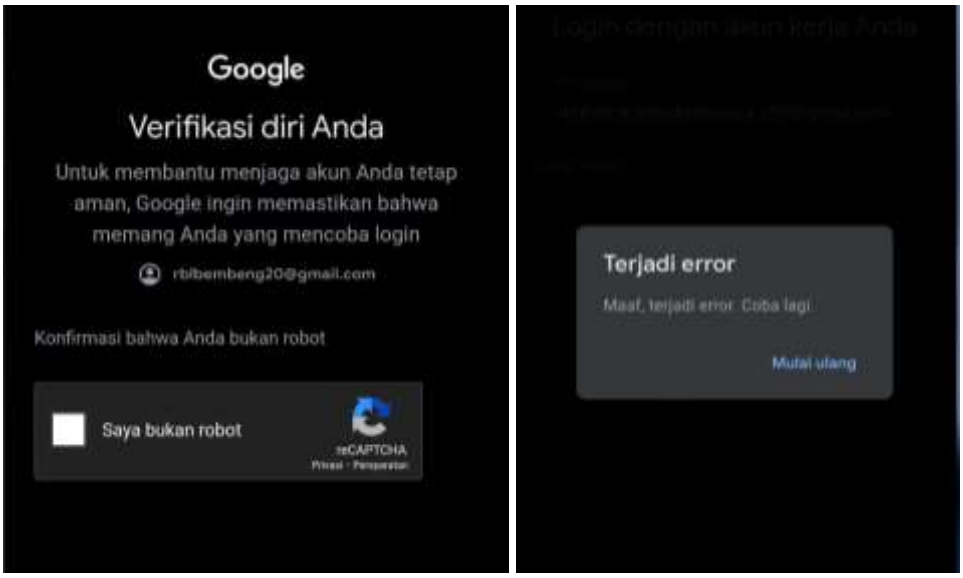
3.3.5 Kata sandi lama



Gambar 9. Kata sandi lama

Dalam kasus ini gambar 9, apabila pengguna telah mengganti kata sandi, peneliti masih memiliki peluang untuk melakukan login dalam kurun waktu hingga tujuh hari menggunakan kata sandi lama. Jika akses berhasil diperoleh dalam rentang waktu tersebut, maka peneliti dapat mengakses seluruh fitur pada akun Gmail target, termasuk melakukan perubahan kata sandi, mengaktifkan fitur keamanan dua langkah (2FA), serta mengelola pengaturan akun lainnya secara menyeluruh.

3.3.6 Batas percobaan

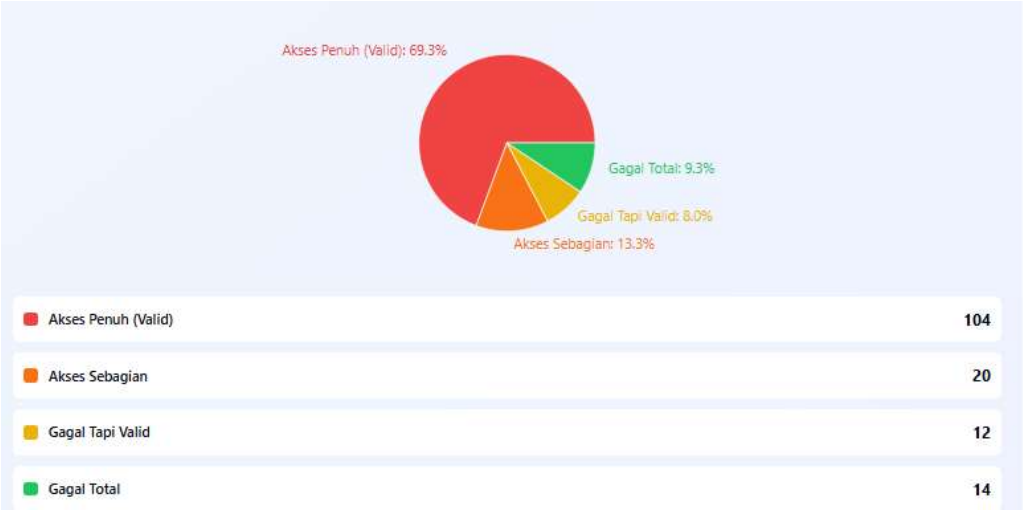


Gambar 10. *Error* percobaan

Penetapan batasan maksimal 15 percobaan *login* per akun dalam penelitian ini didasarkan pada observasi empiris terhadap mekanisme keamanan Gmail yang menerapkan *rate limiting* dan *anomaly detection*. Hasil pengamatan menunjukkan pada gambar 10 bahwa ketika peneliti melakukan percobaan *login* lebih dari 10 kali dalam rentang waktu singkat, sistem Google mulai memicu verifikasi CAPTCHA (reCAPTCHA) untuk memastikan bahwa aktivitas tersebut bukan dilakukan oleh bot otomatis. Selain itu hal itu juga untuk penilaian penetapan oleh peneliti untuk menentukan keberhasilan dalam *Residential Proxy* dalam hal ini.

3.4 Persentase Keberhasilan Serangan

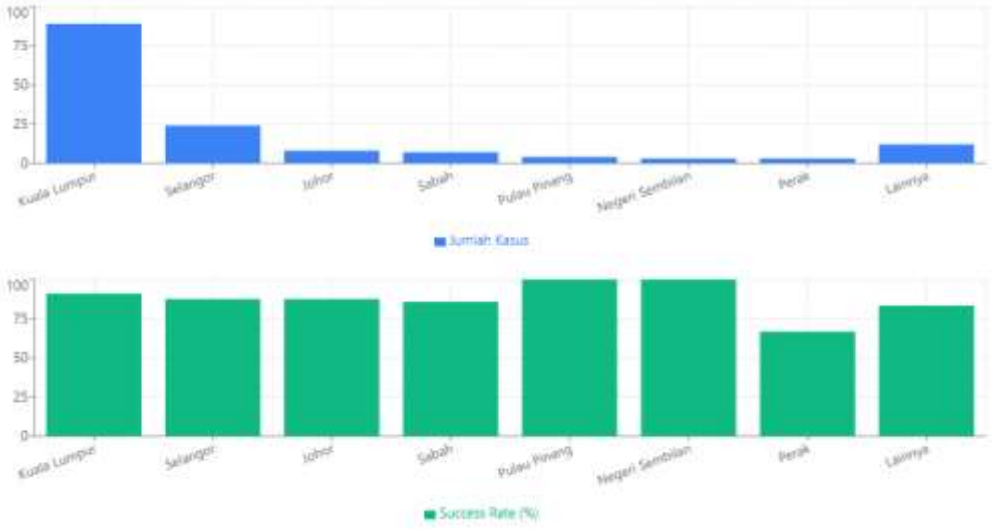
3.4.1 Efektifitas serangan



Gambar 11. Efektifitas Serangan

Gambar 11 menunjukan kemanjuran serangan mencapai 90,7% yang mengesankan (136 dari 150 kasus), dengan 69,3% mencapai akses komprehensif ke data selama percobaan. “Gagal Tapi Valid” kata sandi yang sudah diganti berlaku untuk durasi hingga 7 hari setelah modifikasi menimbulkan interval kerentanan yang cukup besar, memungkinkan peneliti untuk melakukan banyak upaya. Hanya 9,3% serangan yang sama sekali tidak berhasil, menandakan potensi besar dari metode rekayasa sosial yang digunakan dalam inisiatif *phishing* ini.

3.4.2 Distribusi Regional dan Tingkat Keberhasilan per Wilayah



Gambar 12. Sebaran wilayah

Pada gambar 12 Kuala Lumpur mendominasi dengan 59.3% (89 kasus) dan success rate 91%, mengonfirmasi *targeting* pada metropolitan dengan infrastruktur ISP terpusat dan densitas pengguna Gmail tertinggi. Selangor (16%, 24 kasus) dengan success rate 87.5% membentuk zona serangan metropolitan bersama KL. Menariknya, Pulau Pinang dan Negeri Sembilan mencatat *success rate* 100% meskipun volume kecil (4 dan 3 kasus), mengindikasikan bahwa pada wilayah dengan proxy infrastructure yang mature, akurasi teknis lebih dominan daripada volume. Perak menunjukkan *success rate* terendah (66.7%), kemungkinan karena keterbatasan *residential proxy* berkualitas di wilayah tersebut.

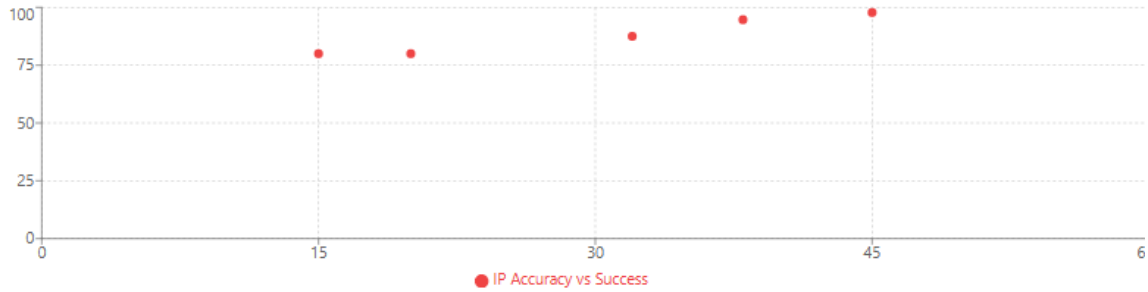
3.4.3 Performa ASN dan Korelasi dengan Tingkat Keberhasilan

Gambar 13. Sebaran ASN

Gambar 13 menjadi sebaran AS4818 (DiGi Telecommunications) mendominasi dengan 52 penggunaan dan success rate tertinggi 92.3%, diikuti AS9534 (Maxis) dengan 37 penggunaan dan 91.9% *success rate*, mengkonfirmasi dominasi tier-1 ISP Malaysia dalam kualitas *residential proxy*. AS4788 (Telekom Malaysia) dengan 31 kasus mencatat 90.3% success rate, menunjukkan performa solid sebagai ISP backbone nasional dengan infrastruktur luas. Ketiga ASN utama ini menguasai 80% total dataset (120 dari 150 kasus), membuktikan bahwa residential proxy dari tier-1 ISP memiliki IP pool besar, geolocation accuracy tinggi, dan *clean reputation*. AS23456 mencatat *success rate* terendah 83.3% dari 18 kasus,

kemungkinan karena *IP reputation* yang lebih rendah, sementara kategori "Lainnya" dengan 12 kasus (91.7%) menunjukkan bahwa diversifikasi ASN minor tetap efektif dalam menghindari *pattern detection*.

3.4.4 Akurasi IP



Akurasi IP	Percobaan	Berhasil	Success Rate
100%	45	44	97.8%
95-99%	38	36	94.7%
90-94%	32	28	87.5%
85-89%	20	16	80%
<85%	15	12	80%
TOTAL	**150**	**136**	90.7%

Gambar 14. Korelasi IP

Data gambar 14 menunjukkan korelasi kuat antara *IP accuracy* dan *success rate*, di mana 100% IP match menghasilkan 97.8% keberhasilan (44 dari 45 percobaan), membuktikan bahwa IP reputation scoring adalah faktor dominan dalam Google authentication system. Penurunan accuracy ke 95-99% masih mempertahankan *success rate* tinggi 94.7%, namun drop signifikan terjadi pada accuracy 90-94% (87.5% success rate) karena sistem mulai mendeteksi anomali. Menariknya, *accuracy* di bawah 85% tetap mencatat 80% *success rate* (12 dari 15), mengindikasikan bahwa kombinasi faktor sekunder (ASN matching, location consistency, port configuration) dapat mengkompensasi IP accuracy yang rendah, terutama jika *residential proxy* menggunakan subnet yang sama (/24 atau lebih besar).

3.5 Fenomena *Window of Vulnerability*

Temuan kritis penelitian ini mengidentifikasi celah keamanan sistematis (*window of vulnerability*) yang muncul dari kebijakan validitas kata sandi lama selama 7 hari. Data menunjukkan 22,13% serangan berhasil pada hari ke-3 hingga ke-6 setelah korban mengganti kata sandi. Periode ini menjadi jendela kritis dimana penyerang masih dapat mengakses sistem menggunakan kredensial yang telah kedaluwarsa.

Fenomena ini memperkuat penelitian Althouse dan Piotrowski (2021) yang menyatakan bahwa kebocoran data masa lalu berdampak jangka panjang jika sistem tidak menerapkan kebijakan *session revocation* yang komprehensif pasca *password reset[16]*. Lebih lanjut, temuan ini mengonfirmasi penelitian Oesch dan Dietrich (2022) tentang keterbatasan MFA sebagai lapisan tunggal tanpa didukung *session management* yang ketat, dimana penyerang dapat memanfaatkan sesi aktif untuk mem-*bypass* autentikasi multi-faktor[17].

3.6 Perbandingan dengan Penelitian Sebelumnya

Dominasi ASN tier-1 Malaysia (AS4818 DiGi, AS9534 Maxis, AS4788 TM) yang secara kolektif menguasai 80% dataset (120 dari 150 kasus) dengan *success rate* konsisten di atas 90%, bukanlah fenomena acak. Temuan kuantitatif ini mengungkap strategi optimasi infrastruktur geolokal yang disengaja oleh penyerang, di mana mereka memanfaatkan *IP pool* dari penyedia layanan utama di wilayah target (Malaysia) untuk meningkatkan akurasi geolokasi dan menghindari deteksi berbasis reputasi IP asing. Pola targeting berbasis ASN ini konsisten dengan evolusi serangan *phishing* modern yang semakin memanfaatkan infrastruktur jaringan terpercaya (*trusted infrastructure*) untuk menembus sistem keamanan. Laporan Cloud Security Alliance (2023) mengkonfirmasi bahwa pemanfaatan teknologi *cloud* dan otomasi telah

memungkinkan peluncuran serangan skala besar dengan presisi tinggi, menggeser paradigma dari serangan *spray-and-pray* massal ke pendekatan yang lebih terukur, personal, dan sulit dilacak karena

menggunakan infrastruktur dengan reputasi bersih[18]. Dalam konteks penelitian ini, penggunaan *residential proxy* dari ASN tier-1 Malaysia berfungsi sebagai *trusted infrastructure* tersebut, yang secara efektif menyamarkan lalu lintas serangan sebagai lalu lintas pengguna lokal yang sah. Lebih lanjut, strategi ini mendapatkan validasi empiris dari korelasi kuat antara akurasi IP dan tingkat keberhasilan yang diungkap dalam penelitian ini. Data menunjukkan bahwa 100% IP match menghasilkan *success rate* 97,8% (44 dari 45 percobaan), sementara akurasi di bawah 85% masih dapat mencapai 80% *success rate* apabila didukung oleh kecocokan ASN dan konsistensi lokasi. Hal ini menunjukkan bahwa dalam ekosistem serangan modern, kecocokan ASN (tier-1) berfungsi sebagai faktor pengkompensasi (*compensating factor*) yang kuat ketika akurasi IP spesifik tidak sempurna. Temuan ini memberikan nuansa penting terhadap penelitian sebelumnya yang mungkin terlalu menekankan akurasi IP absolut sebagai indikator utama. Dominasi wilayah Kuala Lumpur (59,3% kasus dengan *success rate* 91%) dalam dataset semakin memperkuat analisis ini, karena wilayah metropolitan dengan infrastruktur ISP tier-1 yang padat tidak hanya menyediakan *IP pool* yang besar dan beragam, tetapi juga menciptakan "kamuflase" yang ideal bagi lalu lintas serangan untuk menyatu dengan lalu lintas pengguna biasa yang sangat padat.

Kontribusi unik penelitian ini terletak pada identifikasi dan pengukuran kuantitatif terhadap *window of vulnerability* yang diciptakan oleh kebijakan validitas kata sandi lama Google selama 7 hari, di mana 22,1% serangan berhasil pada hari ke-3 hingga ke-6 pasca perubahan kata sandi korban. Temuan temporal ini melengkapi penelitian sebelumnya seperti Guri et al. (2016) yang mengungkap kerentanan dalam proses *password recovery[19]*, namun memberikan kerangka kerja yang lebih terukur mengenai celah eksploitasi yang berkelanjutan. Hasil ini juga memberikan perspektif kritis terhadap narasi industri yang seringkali menempatkan *Multi-Factor Authentication (MFA)* sebagai solusi pamungkas. Penelitian kami menunjukkan bahwa dalam periode *window of vulnerability* ini, ancaman tetap nyata bahkan jika MFA telah diimplementasikan, karena penyerang dapat memanfaatkan sesi yang masih aktif atau melakukan *credential stuffing* sebelum kredensial lama benar-benar dinonaktifkan. Oleh karena itu, temuhan ini menegaskan bahwa strategi penyerangan yang canggih meliputi optimasi geolokal ASN, presisi temporal, dan pemanfaatan *trusted infrastructure* dapat tetap efektif melawan lapisan keamanan tradisional, sehingga memerlukan pendekatan deteksi yang lebih holistik dan proaktif.

4. Kesimpulan

Penelitian ini membuktikan bahwa serangan *phishing* menggunakan *residential proxy* mencapai tingkat keberhasilan 90.7% (136 dari 150 kasus) terhadap akun Gmail di Malaysia, dengan 69.3% memperoleh akses penuh yang memungkinkan pengambilalihan akun secara total. Analisis kuantitatif mengidentifikasi tiga faktor dominan yang menentukan keberhasilan: (1) akurasi IP address dengan korelasi kuat di mana 100% IP match menghasilkan success rate 97.8%, (2) kesesuaian ASN/ISP terutama tier-1 provider Malaysia (AS4818 DiGi 92.3%, AS9534 Maxis 91.9%, AS4788 TM 90.3%) yang menguasai 80% dataset, dan (3) konsistensi lokasi geografis dengan konsentrasi 59.3% serangan di Kuala Lumpur yang mencatat success rate 91%. Temuan kritis mengungkap celah sistemik dalam kebijakan 7-*day old password validity* Google yang menciptakan *window of vulnerability* signifikan, di mana 22.1% serangan berhasil dilakukan 3-6 hari pasca perubahan *password* oleh korban. Pola temporal menunjukkan *strategi wave attack* terkoordinasi dengan *deliberate cooling period* untuk menghindari *detection threshold*, sementara dominasi Gmail (98.7%) mengindikasikan *highly targeted campaign* yang mengeksploitasi kelemahan spesifik ekosistem Google. Penelitian ini berkontribusi pada literatur keamanan siber dengan menyediakan *framework* kuantitatif untuk mengukur efektivitas residential proxy dalam *post-phishing exploitation*, serta merekomendasikan perlunya implementasi mandatory 2FA, pengurangan *validity period password* lama menjadi maksimal 48 jam, dan *enhanced ASN-based anomaly detection* untuk memitigasi ancaman.

5. Daftar Pustaka

[1] A. B. Annef, “Ancaman Siber di Tengah Pandemi Covid-19 : Tinjauan Terhadap Keamanan Non-Tradisional dan Keamanan Siber di Indonesia,” *Sriwijaya Journal of International Relations*, vol. 1, no. 1, 2021, doi: 10.47753/sjir.v1i1.3.

[2] W. A. Karunia, A. Fitya Zahra, and Y. Amrozi, “Kajian Ancaman Baru Dalam Keamanan Informasi: Systematic Literature Review Pada Kerentanan Cyber Security Pasca-Pandemi,” 2025.

[3] X. Mi *et al.*, “Resident evil: Understanding residential IP proxy as a dark service,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2019. doi: 10.1109/SP.2019.00011.

[4] N. S. Zaini *et al.*, “Phishing detection system using machine learning classifiers,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, 2020, doi: 10.11591/ijeecs.v17.i3.pp1165-1171.

[5] T. Mehraj, M. A. Sheheryar, S. A. Lone, and A. H. Mir, "A critical insight into the identity authentication systems on smartphones," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 3, 2019, doi: 10.11591/ijeecs.v13.i3.pp982-989.

[6] M. Guri, E. Shemer, D. Shirtz, and Y. Elovici, "Personal information leakage during password recovery of internet services," in *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*, 2017. doi: 10.1109/EISIC.2016.035.

[7] G. Mogos and N. S. Mohd Jamail, "Study on security risks of e-banking system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 2, 2020, doi: 10.11591/ijeecs.v21.i2.pp1065-1072.

[8] E. Chiapponi, M. Dacier, and O. Thonnard, "Inside Residential IP Proxies: Lessons Learned from Large Measurement Campaigns," in *Proceedings - 8th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2023*, 2023. doi: 10.1109/EuroSPW59978.2023.00062.

[9] M. N. Trisolvena and N. H. Saputra, "Phishing Cyber Security Threats," *Jurnal Improsci*, vol. 2, no. 1, pp. 38–48, Aug. 2024, doi: 10.62885/improsci.v2i1.440.

[10] D. Komosny, M. Voznak, and S. U. Rehman, "Location accuracy of commercial IP address geolocation databases," *Information Technology and Control*, vol. 46, no. 3, 2017, doi: 10.5755/j01.itc.46.3.14451.

[11] Z. Wang, Y. Niu, H. Chen, G. Cheng, J. Cui, and Z. Zhang, "Target driven IP Geolocation Algorithm," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1861/1/012002.

[12] D. Firewall *et al.*, "Implementasi Keamanan Hotspot Menggunakan Proxy," *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, vol. 8, no. 2, pp. 148–154, 2022.

[13] M. Campobasso and L. Allodi, "Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2020. doi: 10.1145/3372297.3417892.

[14] Suci Sekar Sari and Agus Tedyyana, "Analisis Efektivitas Rule Snort dalam Mendeteksi Serangan Jaringan," *Repeater : Publikasi Teknik Informatika dan Jaringan*, vol. 2, no. 4, pp. 01–15, Aug. 2024, doi: 10.62951/repeater.v2i4.194.

[15] M. Nasution, M. Haris Munandar, and E. P. Korespondensi, "JURNAL MEDIA INFORMATIKA [JUMIN] Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan IDS pada Infrastruktur Jaringan Skala Kecil-Menengah," 2025.

[16] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Comput Secur*, vol. 108, p. 102355, 2021, doi: https://doi.org/10.1016/j.cose.2021.102355.

[17] S. Hessien and M. Hassan, "PISCOT: A Pipelined Split-Transaction COTS-Coherent Bus for Multi-Core Real-Time Systems," *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 1, Oct. 2022, doi: 10.1145/3556975.

[18] A. Sikorski, L. Pavlova, D. Martin, and J. Gil, "Laonice (Sarsiana) sinica Sikorski & Wu 1998," May 2023, *Zenodo*. doi: 10.5281/zenodo.7890123.

[19] M. Guri, E. Shemer, D. Shirtz, and Y. Elovici, "Personal Information Leakage During Password Recovery of Internet Services," in *2016 European Intelligence and Security Informatics Conference (EISIC)*, 2016, pp. 136–139. doi: 10.1109/EISIC.2016.035.