Jurnal Elektronika dan Teknik Informatika Terapan (JENTIK)
Vol. 4 No. 1 Maret 2026
e-ISSN : 2988-0874 p-ISSN : 2988-0866, Hal 01-13
DOI: https://doi.org/10.59061/jentik.v4i1.1386
Tersedia: https://e-journal.poltek-kampar.ac.id/index.php/JENTIK

Pemetaan dan Analisis Permukaan Serangan (Attack Surface) Sistem Elektronik Pemerintah Daerah Melalui Identifikasi Subdomain Resmi

Safni Marwa [1], Slamet Triyanto[2*], Andri Nofiar. Am[3]
[1] Universitas Pahlawan Negara, Indonesia
[2] Dinas Komunikasi Informatika dan Persandian Kabupaten Kampar, Indonesia
[3] Politeknik Negeri Bengkalis, Indonesia
Email: safnimarwa@universitaspahlawan.ac.id[1], slamettriyanto@staff.kamparkab.go.id[2], andrinofiar90@gmail.com[3]

Penulis Korespondensi: slamettriyanto@staff.kamparkab.go.id

Abstract. *The number of cyberattack incidents recorded by the Badan Siber dan Sandi Negara (BSSN) reached 3.64 million by mid-2025. The majority of these incidents targeted government systems. As of June 2023, Riau Province, which comprises 12 regencies and municipalities, recorded the highest number of incidents among governmental institutions in Indonesia, totaling 54,313,225 cases. The results of domain and subdomain scanning conducted across Riau Province and its regencies/municipalities identified 5,252 public electronic systems. Among these, a significant portion consisted of inactive domains or parking domains, installer pages, landing pages, expired SSL certificates, development pages, and systems potentially utilizing outdated technologies. Although the use of obsolete technologies cannot be conclusively confirmed, this indication is reflected in the number of domains and subdomains affected by web defacement incidents.To ensure that the research process did not violate applicable legal and ethical standards, domain and subdomain scanning and examination were conducted exclusively using publicly available tools, such as web browsers and Subfinder. Furthermore, no deeper penetration testing was performed on the identified findings. This limitation justifies the unavailability of definitive information regarding the use of outdated systems. Finally, asset identification constitutes a crucial stage, enabling the implementation of further measures for incident handling and mitigation efforts aimed at preventing future cyber incidents.*

Keywords: *Cyber Incidents; Digital Asset Identification; Domain Scanning; Domain; Subdomain.*

Abstrak. Insiden serangan siber yang tercatatat oleh Badan Siber dan Sandi Negara (BSSN) hingga pertengahan 2025 mencapai 3,64 juta. Insiden ini sebagian besar menyasar ke sistem Pemerintahan. Provinsi Riau dengan 12 Kabupaten/Kota yang berada dalam wilayahnya per Juni 2023 menjadi Lembaga pemerintahan yang mengalami insiden terbanyak di Indonesia mencapai 54.313.225 kali. Dari hasil pemindaian terhadap domain dan subdomain Provinsi Riau dan Kabupaten Kota yang ada di dalamnya memiliki sistem elektronik publik 5252 sistem. Dengan jumlah ini, Sebagian domain merupakan domain tidak aktif / parking domain, halaman installer, landing page, SSL expired, dan halaman development termasuk penggunaan perangkat usang. Meskipun belum dapat dipastikan tentang penggunaan teknologi usang, namun indikator ini dapat dilihat dari jumlah domain maupun sub domain yang terserang web deface. Untuk memastikan proses penelitian tidak melanggar norma maupun hukum yang berlaku, maka proses pindai dan pemeriksaan domain dan sub domain menggunakan perangkat lunak publik seperti perambah internat dan subfinder. Selain itu juga tidak dilakukan penetrasi lebih dalam terhadap temuan yang diperoleh, hal ini juga menjadi justifikasi tidak tersedianya informasi sistem yang digunakan telah usang. Selanjutnya, idetifikasi aset merupakan tahapan yang sangat dibutuhkan sehingga berbagai Langkah lanjutan dapat di dilakukan sebagai bentuk penanganan insiden maupun proses mitigasi untuk mencegah insiden siber lebih lanjut.

Kata Kunci: Domain; Identifikasi Aset Digital; Insiden Siber; Pemindaian Domain; Subdomain.

1. LATAR BELAKANG

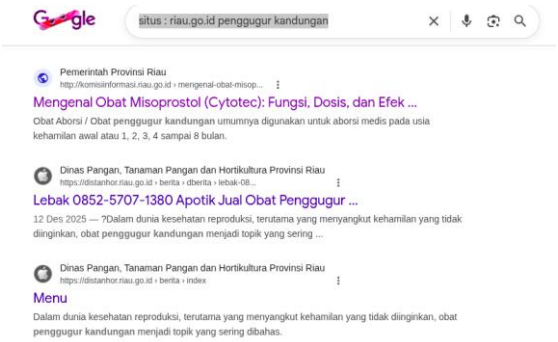
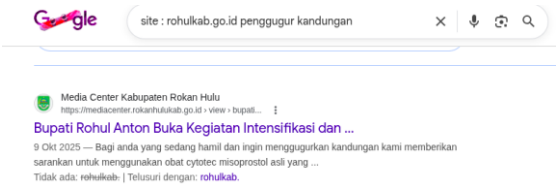
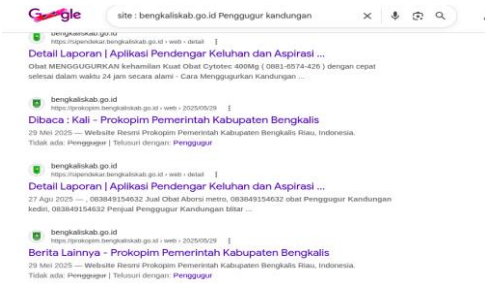
Laporan dari Badan Siber dan Sandi Negara (BSSN) yang dimuat oleh tempo (Dhanya, 2025) menunjukkan bahwa hingga Juli 2025 terdapat serangan siber sebanyak 3,64 juta insiden. Jumlah ini setara dengan insiden siber dalam kurun waktu 5 (lima) tahun terakhir (Dhanya, 2025). Sedangkan data dari laporan tahunan layanan honeynet BSSN (BSSN, 2023) yang dimuat dalam artikel cnn Indonesia, Provinsi dengan jumlah serangan siber terbesar pada

Naskah Masuk: 12 Januari 2025; Revisi: 07 Februari 2026; Diterima: 13 Maret 2026; Terbit: 16 Maret 2026

tahun 2023 adalah Provinsi Riau (Indonesia, 2023). tercatat hingga 09 Juni 2023 Provinsi Riau mendapat serangan siber hingga 54.313.225 kali (Indonesia, 2023).

Besarnya insiden siber yang terjadi di Provinsi Riau, sedianya sudah dapat dipetakan sejak dini, mengingat jika merujuk ke Grand Design Riau Digital Provinsi Riau 2021-2025 aspek keamanan juga telah menjadi prioritas dalam kegiatan digitalisasi Provinsi (Riau, 2021). Namun hasil dari pencarian dengan menggunakan kata kunci seperti slot or gacor, penggugur kandungan, slot 88 dan lain-lain (Woncharso et al., 2021), yang merupakan trend insiden web deface pada system go.id (Nurseno et al., 2024) menunjukkan bahwa system elektronik yang ada Provinsi riau dan Kabupaten Kota yang ada di dalamnya masih sangat banyak mengalami insiden ini. Pencarian per Januari 2025 menggunakan google search engine Tabel 1 menunjukkan bahwa insiden web deface masih sangat tinggi di Provinsi Riau.

Tabel 1 Tangkapan Google Search Web Deface.

No	Kata Kunci	Tangkapan Layar
1.	situs: riau.go.id penggugur kandungan	
2.	site: rohulkab.go.id penggugur kandungan	
3.	site: bengkaliskab.go.id Penggugur kandungan	

Sumber data: primer

Beberapa Tindakan pencegahan sepertinya juga telah dilakukan dengan adanya Kabupaten Kota yang tidak terdeteksi *deface*, namun jika di telaah lebih jauh sistem elektronik yang terdapat di Kabupaten/Kota tersebut tidak terdaftar pada mesin pencari seperti google.com. Padahal media paling umum untuk mencari layanan publik bagi Masyarakat adalah dengan menggunakan *search engine* (Woncharso et al., 2021).

Meskipun tidak ada Teknik yang benar-benar baku dan efektif untuk melakukan penanganan insiden siber (Aji et al., 2025), Hal yang sangat perlu dilakukan agar keamanan meningkat adalah pembaruan perangkat lunak yang digunakan (Aryapranata et al., 2024). Permasalahan muncul Ketika sistem elektronik yang ada tidak terdata dengan baik, atau bahkan tidak diketahui keberadaanya sehingga banyak aset yang tidak terkelola dan sulit untuk dilakukan proses pembaruan yang mengakibatkan adanya celah keamanan siber (Aryapranata et al., 2024).

Dalam mendeteksi aset yang ada di sautu organisasi, penyerang ataupun *red team* biasanya mengecek jumlah aset yang tersedia dan dapat diakses secara umum atau biasa disebut dengan *External Attack Surface* (EAS)(Q Fadlan, 2025). EAS biasanya memanfaatkan perangkat *open source intelligence* (OSINT) seperti subfinder (Q Fadlan, 2025). Subfinder dari laman resmi github.com tempat dipublikasikannya perangkat ini, menyatakan bahwa perangkat lunak ini dikembangkan untuk melakukan penelitian atau pekerjaan internal (projectdiscovery.io, 2025). Dengan klaim ini, maka penggunaan subfinder sedianya tidak menjadi perangkat lunak yang bertentanganan secara hukum jika digunakan untuk melakukan penelitian.

2. KAJIAN TEORITIS

Melakukan inventarisir aset teknologi merupakan pondasi dalam upaya pertahanan keamanan siber (Asia, 2026). Identifikasi aset ini tidak hanya sekedar melakukan pengecekan namun juga manajemen aset sehingga dapat memperkecil dampak yang ditimbulkan dari serangan siber (Nurhidayat et al., 2024). National Institute of Standards and Technology (NIST) membuat katogori aset menjadi 3 (tiga) bentuk yakni aset fisik, non fisik dan manusia (The NIST Cybersecurity Framework (CSF) 2.0, 2024). Dengan bentuk aset ini, maka inventarisi aset bukan hanya sebagai tahapan untuk mendata namun juga memastikan semua aset terpantau (Asia, 2026). Adapun aset yang dapat di data dan dipantau diatanranya adalah data, hardware, sistem, fasilitas, layanan dan manusia (The NIST Cybersecurity Framework (CSF) 2.0, 2024). Selanjutnya secara spesifik itsec.id menjabarkan aset digital yang memerlukan identifikasi meliputi endpoint (seperti laptop, server dan perangkat selular),

Infrastruktur jaringan (diataranya Router, Switch, Firewall dan lain-lain), Cloud dan Aplikasi, dan aset external (domain website, Alamat IP, dan API).

Indentifikasi aset seperti domain website, dapat dilakukan dari ranah public atau biasa disebut dengan OSINT (Q Fadlan, 2025). OSINT dapat diartikan sebagai upaya mengumpulkan informasi dari area publik, kemudian informasi tersebut dikumpulkan dianalisis dan disebarluaskan (Raharja, 2024). Dengan justifikasi OSINT mengumpulkan informasi dari ranah publik maka tidak ada larangan dan tidak akan menggangu proses bisnis dari organisasi. Pada domain website Pemerintah (go.id) merupakan area yang paling sering dijadikan gerbang untuk melakukan serangan siber. Terbukti dari temuan 2.090.000 situs web dengan domain .go.id terkena serangan judi online (Fadli Mutaqin & Ferdiansyah, 2022). Teknik yang digunakan untuk menemukan informasi ini tidak menggunakan metode aktif seperti pemindaian dengan brute force, namun dengan menggunakan google dork (Raharja, 2024).

Selain memanfaatkan perangkat mesin pencari seperti google dork, alat lain yang dapat digunakan untuk mengumpulankan informasi publik nama domain website adalah subfinder (Q Fadlan, 2025). Subfinder pada proses kerjanya tidak melakukan pemindaian aktif (projectdiscovery.io, 2025). Perangkat yang dibuat dan dikembangkan oleh projectdiscovery ini memanfaatkan data dari sumber osint (projectdiscovery.io, 2025). Pada halaman disclaimer disebutkan bahwa subfinder memanfaatkan API dari berbagai sumber terbuka seperti Bufferover, CommonCrawl, certporter, dnsdumster, google transparency, alienvault (projectdiscovery.io, 2025). Cara kerja dari subfinder setidaknya terdiri atas 3 (tiga) tahapan yakni mengumpulkan data dari sumber OSINT, melakukan query dari berbagai sumber API, parsing dan normalisasi data (projectdiscovery.io, 2023).

Melakukan inventarisir aset teknologi merupakan pondasi dalam upaya pertahanan keamanan siber (Asia, 2026). Identifikasi aset ini tidak hanya sekedar melakukan pengecekan namun juga manajemen aset sehingga dapat memperkecil dampak yang ditimbulkan dari serangan siber(Nurhidayat et al., 2024). National Institute of Standards and Technology (NIST) membuat katogori aset menjadi 3 (tiga) bentuk yakni aset fisik, non fisik dan manusia (The NIST Cybersecurity Framework (CSF) 2.0, 2024). Dengan bentuk aset ini, maka inventarisasi aset bukan hanya sebagai tahapan untuk mendata namun juga memastikan semua aset terpantau (Asia, 2026). Adapun aset yang dapat di data dan dipantau diatanranya adalah data, hardware, sistem, fasilitas, layanan dan manusia (The NIST Cybersecurity Framework (CSF) 2.0, 2024). Selanjutnya secara spesifik itsec.id menjabarkan aset digital yang memerlukan identifikasi meliputi endpoint (seperti laptop, server dan perangkat selular),

Infrastruktur jaringan (diataranya Router, Switch, Firewall dan lain-lain), Cloud dan Aplikasi, dan aset external (domain website, Alamat IP, dan API).

Indentifikasi aset seperti domain website, dapat dilakukan dari ranah publik atau biasa disebut dengan OSINT (Q Fadlan, 2025). OSINT dapat diartikan sebagai upaya mengumpulkan informasi dari area publik, kemudian informasi tersebut dikumpulkan dianalisis dan disebarluaskan(Raharja, 2024). Dengan justifikasi OSINT mengumpulkan informasi dari ranah publik maka tidak ada larangan dan tidak akan menggangu proses bisnis dari organisasi. Pada domain website Pemerintah (go.id) merupakan area yang paling sering dijadikan gerbang untuk melakukan serangan siber. Terbukti dari temuan 2.090.000 situs web dengan domain .go.id terkena serangan judi online (Fadli Mutaqin & Ferdiansyah, 2022). Teknik yang digunakan untuk menemukan informasi ini tidak menggunakan metode aktif seperti pemindaian dengan brute force, namun dengan menggunakan google dork yang merupakan Teknik pasif dalam pemindaian (Raharja, 2024).

Selain memanfaatkan perangkat mesin pencari seperti google dork, alat lain yang dapat digunakan untuk mengumpulankan informasi publik nama domain website adalah Subfinder (Q Fadlan, 2025). Subfinder pada proses kerjanya tidak melakukan pemindaian aktif (projectdiscovery.io, 2023). Perangkat yang dibuat dan dikembangkan oleh projectdiscovery ini memanfaatkan data dari sumber OSINT (projectdiscovery.io, 2025). Pada halaman disclaimer disebutkan bahwa subfinder memanfaatkan Application Programmable Interface (API) dari berbagai sumber terbuka seperti Bufferover, CommonCrawl, certporter, dnsdumster, google transparency, alienvault (projectdiscovery.io, 2025). Cara kerja dari subfinder setidaknya terdiri atas 3 (tiga) tahapan yakni mengumpulkan data dari sumber OSINT, melakukan query dari berbagai sumber API, parsing dan normalisasi data (projectdiscovery.io, 2023).

Provinsi Riau secara administrasi memiliki 12 Kabupaten/Kota (Badan Pusat Statistik Provinsi Riau, 2024). Sesuai dengan pembagian administratif, Provinsi dan Kabupaten/Kota yang ada juga memiliki identitas dalam dunia siber yang disebut dengan website (Utami, 2022). Website yang dimiliki tiap daerah memiliki ciri khas nama yang berbeda yang kemudian disebut dengan domain website. Tabel 2 merupakan list nama Kabupaten/Kota yang ada di Provinsi Riau dan Nama domain pada tiap wilayah.

Domain website atau nama domain merupakan identitas dari suatu Lembaga, dalam konteks penelitian merupakan Lembaga yang dimaksud adalah pemerintah (PENGGUNAAN NAMA DOMAIN Go.Id UNTUK SITUS WEB RESMI PEMERINTAHAN PUSAT DAN DAERAH, 2006). Idealnya kepemilikan sistem elektronik (SE) diberi nama sesuai dengan

nama domain sedangkan untuk nama domain yang berada dibawahnya harus merujuk kepada nama domain induk (PENGGUNAAN NAMA DOMAIN Go.Id UNTUK SITUS WEB RESMI PEMERINTAHAN PUSAT DAN DAERAH, 2006) . Sehingga diketahui bahwa SE yang berjalan merupakan benar dan sah dari pemilik sistem.

Sesuai dengan peraturan Menteri kominfo bahwa nama domain pemerintah wajib menggunakan go.id (PENGGUNAAN NAMA DOMAIN Go.Id UNTUK SITUS WEB RESMI PEMERINTAHAN PUSAT DAN DAERAH, 2006). Sehingga semua semua sistem elektronik yang berada di bawah dari naungan Lembaga harus merujuk pada domain induk (PENGGUNAAN NAMA DOMAIN Go.Id UNTUK SITUS WEB RESMI PEMERINTAHAN PUSAT DAN DAERAH, 2006).

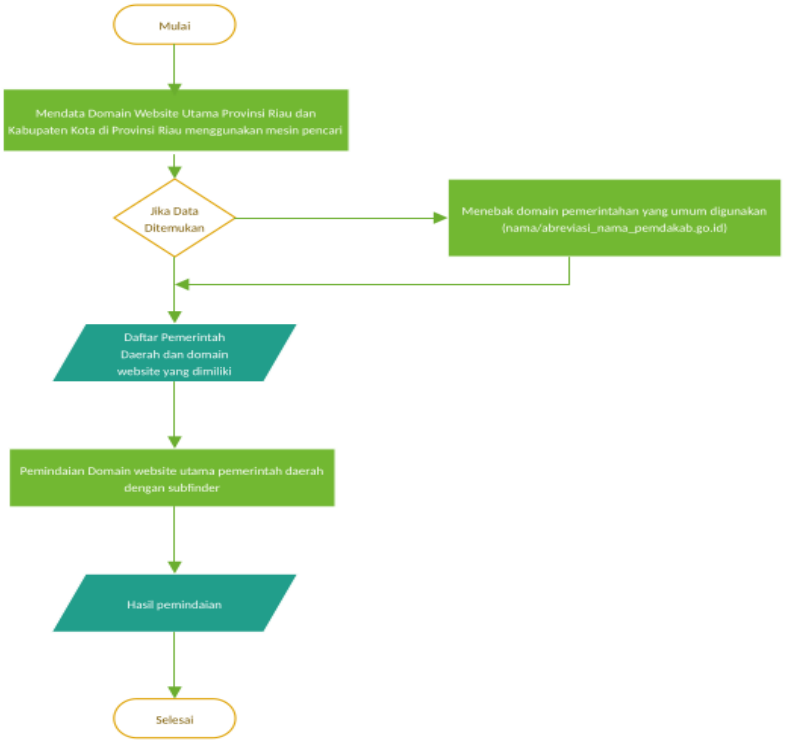
Tabel 2 Nama Domain Pemerintah Provinsi dan Kabupaten/Kota di Riau.

No	Wilayah Administrasi	Domain Website
1.	Provinsi Riau	https://riau.go.id
2.	Bengkalis	https://bengkaliskab.go.id
3.	Indragiri Hilir	https://www.inhilkab.go.id
4.	Indragiri Hulu	https://inhukab.go.id
5.	Kampar	https://kamparkab.go.id
6.	Kuantan Singingi	https://kuansing.go.id
7.	Pelalawan	https://pelalawankab.go.id
8.	Rokan Hulu	https://rokanhulukab.go.id
9.	Siak	https://siakkab.go.id
10.	Dumai	https://dumaikota.go.id
No	Wilayah Administrasi	Domain Website
11.	Kepulauan Meranti	https://merantikab.go.id
12.	Pekanbaru	https://pekanbaru.go.id
13.	Rokan Hilir	https://rohilkab.go.id

Sumber data: primer

3. METODE PENELITIAN

Penelitian memanfaatkan tools OSINT Subfinder untuk memindai domain dan subdomain yang ada di Provinsi Riau dan Kabupaten/Kota yang ada di dalamnya. Langkah pertama yang dilakukan adalah membuat daftar domain utama milik Pemerintah yang menjadi objek penelitian. Selanjutnya melakukan pemindaian domain website tersebut. Hasil dari pemindaian dimuat dalam bentuk data spradsheet/excel untuk menampilkan jumlah domain website yang ada. Tahapan terakhir adalah menghitung jumlah nama sub domain pada tiap daerah untuk menjadi rujukan jumlah SE yang aktif maupun tidak aktif.



Gambar 1. Diagram Alur Penelitian.

Penghitungan jumlah sub domain pada tiap daerah digunakan sebagai penghitungan jumlah layanan pada daerah tersebut. Selain itu juga sebagai acuan kemungkinan tata Kelola sistem elektronik yang dimiliki. Selain menghitung jumlah SE dari nama domain dan sub domain, pengambilan sampel dari tiap temuan pemindaian pada tiap daerah juga dilakukan. Pengambilan sampel dengan mengambil tangkapan layer SE untuk memastikan bahwa sub domain maupun domain masih dalam kondisi aktif. Sedangkan variabel yang digunakan untuk menentukan sampel sebagai SE aktif atau tidak hanya dari satu variabel yakni pembaharuan konten dari SE. Dengan justifikasi ini juga menjadi ketentuan bahwa penelitian tidak akan melakukan pengujian penetrasi pada sistem yang dijadikan sampel.

Pada tahap pemilihan sampel, dilakukan secara acak dan hanya melihat nama domain yang pertama kali muncul Ketika melakukan pemindaian dengan subfinder. Meskipun tidak menutup kemungkinan pada tiap kali pemindaian akan menampilkan nama sub domain yang berbeda. Namun demikian dengan pemilihan secara acak menjadi justifikasi selanjutnya tentang obyektifitas dari penelitian yang dilakukan.

4. HASIL DAN PEMBAHASAN

Sesuai dengan tahapan dalam diagram alur penelitian, proses pendataan nama domain utama merupakan hal pertama yang dilakukan. Data primer berisi nama domain dan nama pemerintahan terdapat pada table 2. Selanjutnya lakukan perintah subfinder pada tiap domain yang sudah terdapat dengan perintah "subfinder -d riau.go.id -o prov_riau.txt". Perintah ini dijalankan pada terminal kali linux yang terinstall subfinder. Makna dari perintah tersebut yakni jalan subfinder pada domain riau.go.id dengan keluaran prov_riau.txt.

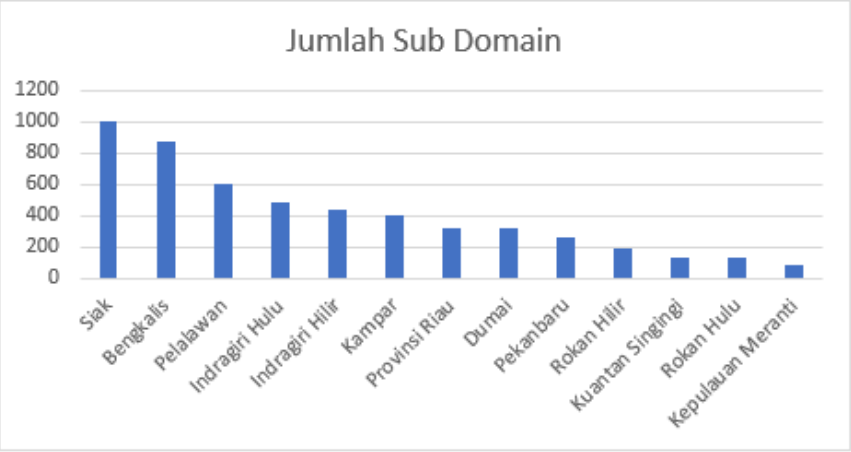
Dari hasil subfinder diperoleh informasi Provinsi Riau dan Kabupaten Kota yang ada di dalam Provinsi memiliki total sub domain 5252 Sub Domain. Dengan pembagian sebagai berikut:

Tabel 3 Jumlah Sub Domain Tiap Daerah.

NO	Daerah	Jumlah Sub Domain
1	Provinsi Riau	322
2	Bengkalis	877
3	Indragiri Hilir	436
4	Indragiri Hulu	486
5	Kampar	405
6	Kuantan Singingi	132
7	Pelalawan	607
8	Rokan Hulu	126
9	Siak	1008
10	Dumai	317
11	Kepulauan Meranti	85
12	Pekanbaru	261
13	Rokan Hilir	190

Sumber data : primer

Dari tabel terlihat bahwa pemilik sub domain terbanyak di Provinsi Riau adalah Kabupaten Siak dengan 1008 sub domain disusul Kabupaten Bengkalis 877 sedangkan Pemilik sub domain paling sedikit adalah Kabupaten Kepulauan Meranti dengan 85 Sub Domain.



Gambar 2 Pemilik Sub Domain di Provinsi Riau.

Sesuai dengan rencana penelitian, dilakukan pengecekan terhadap domain yang pertama kali muncul pada saat dilakukan pemindaian dengan *subfinder*. Pemilihan sampel terhadap 5 (lima) domain yang pertama muncul diharapkan menjadikan penelitian lebih obyektif. Tabel 4 merupakan 5 (lima) sub domain pertam ahasil pindai *subfinder*.

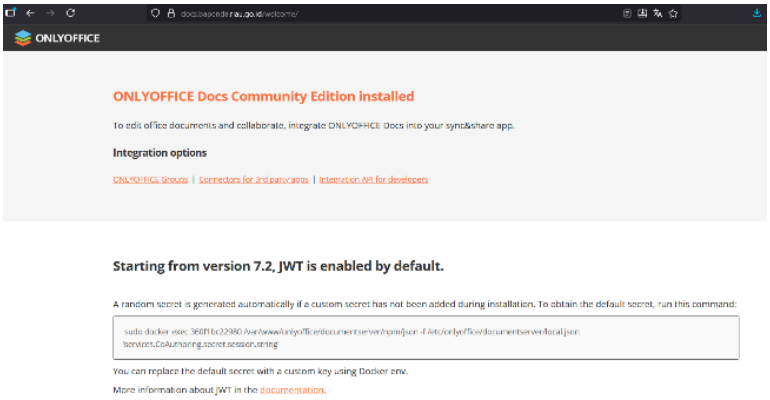
Tabel 4 LIma List sub domain pertama hasil pindai subfinder.

No	Daerah	Sub Domain
1	Provinsi Riau	docs.bapenda.riau.go.id
		sikepo.dispora.riau.go.id
		okkpd.distanhor.riau.go.id
		ppdisnakertrans.riau.go.id
		silaris.riau.go.id
2	Bengkalis	78f7b20b59e8bc97fcbf7ff4e3e032fb-esign-client.bengkaliskab.go.id
		developcakeb.bengkaliskab.go.id
		klikbermasa.bengkaliskab.go.id
		mpp.bengkaliskab.go.id
		muarabasung.bengkaliskab.go.id
3	Indragiri Hilir	gembira.desa.inhilkab.go.id
		sungaiterab.desa.inhilkab.go.id
		datacenter-dinkes.inhilkab.go.id
		belarasbarat.desa.inhilkab.go.id
		bentengbarat.desa.inhilkab.go.id
4	Indragiri Hulu	dpupr.inhukab.go.id
		www.bakohumas.inhukab.go.id
		webmail.simpatda.inhukab.go.id
		webmail.kominfo.inhukab.go.id
		mail.disnakkan.inhukab.go.id
5	Kampar	app.rsudbangkinang.kamparkab.go.id
		swara.kamparkab.go.id
		webmail.bkd.kamparkab.go.id
		plan.kamparkab.go.id
		e-planing.kamparkab.go.id
6	Kuantan Singingi	mail.kuansing.go.id
		simpan-spbe.kuansing.go.id
		diskominfoss.kuansing.go.id
		pkm-sentajo.kuansing.go.id
		sidodadi.kuansing.go.id
7	Pelalawan	disarpus.pelalawankab.go.id
		www.opendata.laksa.pelalawankab.go.id
		mail.sibadik.pelalawankab.go.id
		cpanel.newsibadik.pelalawankab.go.id
		mail.monev.pelalawankab.go.id
8	Rokan Hulu	dkpp.rokanhulukab.go.id
		rambahtengahhilir.rokanhulukab.go.id
		box.rokanhulukab.go.id
		rambahhilir.rokanhulukab.go.id

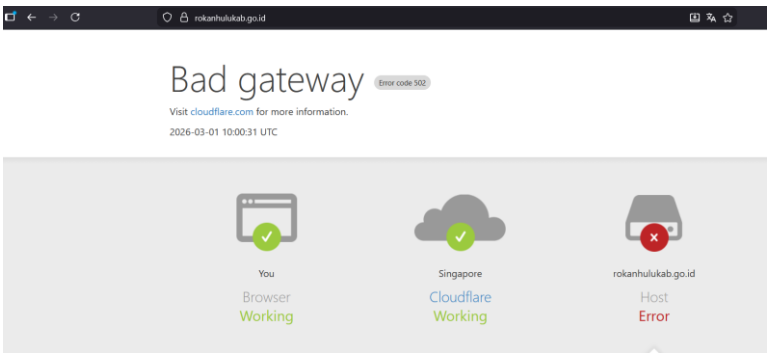
		www.agenda.rokanhulukab.go.id
9	Siak	cpcontacts.silawa.siakkab.go.id
		webdisk.sikda.siakkab.go.id
		sipadu.siakkab.go.id
		cpanel.sipeta.siakkab.go.id
		cpcalendars.desa-penyengat.siakkab.go.id
10	Dumai	kec-sungaisembilan.dumaikota.go.id
		mail.bansos-siaga.dumaikota.go.id
		cpcontacts.dishub.dumaikota.go.id
		webdisk.sijabpri.dumaikota.go.id
		disnakkanla.dumaikota.go.id
11	Kepulauan Meranti	pulaumerbau.merantikab.go.id
		sempolet.merantikab.go.id
		sidp.merantikab.go.id
		sintal.merantikab.go.id
		smartcity.merantikab.go.id
12	Pekanbaru	appdukcapil.pekanbaru.go.id
		adpum.pekanbaru.go.id
		sitangan-disketapang.pekanbaru.go.id
		www.iumk.pekanbaru.go.id
		agendawako.pekanbaru.go.id
13	Rokan Hilir	lensa.rohilkab.go.id
		ptsp.rohilkab.go.id
		cpanel.bkpsdm.rohilkab.go.id
		ftp.jdih.rohilkab.go.id
		dlhrohil.rohilkab.go.id

Sumber data : primer

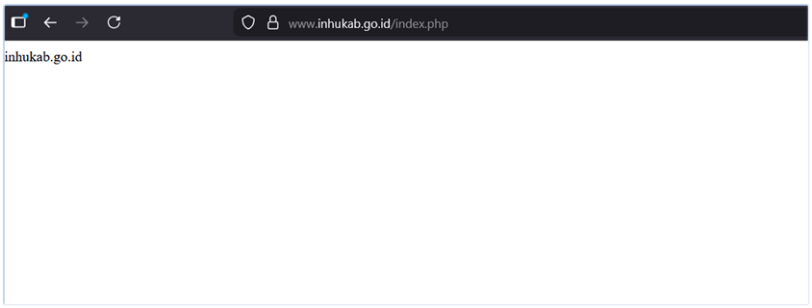
Setelah dilkukan penelitian ternyata masih terdapat banyak sekali domain yang tidak aktif / *parking domain*, halaman installer, landing page dan masih banyak lagi informasi yang menunjukkan bahwa domain dibuat namun tidak pernah benar-benar digunakan. Penelitian ini tidak menyertakan semua tangkapan layer pada saat penelitian dilakukan dan belum dilakukan pengecekan lebih lanjut mengenai kondisi pada tiap domain Ketika diakses menggunakan browser. Namun dari penamaan sub domain masih terdapat banyak yang merupakan halaman *dev* yang sedianya tidak ditempatkan sebagai domain *go live*. Beberapa Kabupaten/Kota pada domain induk per tanggal 1 Maret 2026 dalam kondisi tidak aktif atau di redirect ke halaman lain seperti Kabupaten Rokan Hulu yang domain utama tidak aktif atau kesulitan untuk untuk diakses. Sedangkan kabupaten Indragiri Hulu www.inhukab.go.id masih menampilkan *landing page*.



Gambar 3 Tangkapan layar https://docs.bapenda.riau.go.id.



Gambar 4 Halaman domain utama rokanhulukab.go.id.



Gambar 5 Tangkapan Layar www.inhukab.go.id.

Selain berbagai tantangan yang telah disebutkan, permasalahan lain yang langsung dapat dilihat adalah sertifikat Secure Socket Layers (SSL) yang telah kadaluarsa. Hal ini dapat menjadi celah keamanan siber yang serius apa lagi jika SSL diterapkan pada domain utama yang merupakan marwah pada institusi Pemerintah Daerah.

5. KESIMPULAN DAN SARAN

Berbagai tantangan dalam pembenahan aset digital masih sangat banyak, proses pembenenahan asset merupakan hal mutlak yang harus dilakukan. Mitigasi akan insiden siber merupakan tahapan yang jauh lebih efektif di bandingkan dengan jika harus melakukan perbaikan paska insiden. Meskipun dalam penelitian menggunakan sampel dari Provinsi Riau, namun kondisi serupa diyakini juga terjadi pada Lembaga Pemerintah lainnya di Indonesia.

Permasalahan yang ditemukan dari hasil penelitian menunjukkan bahwa Sistem Elektronik (SE) Pemerintah dari sisi pemeriksaan domain masih banyak yang tidak aktif / *parking domain*, halaman installer, *landing page*, *SSL expired*, dan halaman *development* meskpun kondisi SE sudah *go live*. Selain itu penerapan *clean code* sangat dibutuhkan untuk memastikan SE yang telah go live benar-benar telah melewati tahap *testing* yang tepat. Hal ini dikarenkan SE merupakan aset yang juga membutuhkan pembiayaan dalam tahap pembuatan maupun pasca sistem *go live*.

DAFTAR REFERENSI

Aji, B. B., Alimyaningtias, W. N., Abdillah, M. F., Satrio, D., Utomo, I., & Artikel, H. (2025). Tinjauan keamanan terhadap serangan deface website sebagai bentuk cybercrime. *JAITS: Journal of Applied Information Technology Solution, 2*(1), 7–11. https://journal.universitasmulia.ac.id/index.php/jaits

Aryapranata, A., Hermanto, S., Agsena, Y. P., Rasyid, Y. Al, & Habibie, F. H. (2024). Pencegahan web defacement. *Jurnal Esensi Infokom: Jurnal Esensi Sistem Informasi Dan Sistem Komputer, 8*(1), 10–19. https://doi.org/10.55886/infokom.v8i1.816

Asia, I. (2026). Mengapa inventaris aset adalah fondasi pertahanan siber yang kuat. https://itsec.id/blog/mengapa-inventaris-aset-adalah-fondasi-pertahanan-siber-yang-kuat

Badan Pusat Statistik Provinsi Riau. (2024). Nama ibukota kabupaten/kota di Provinsi Riau. https://riau.bps.go.id/id/statistics-table/1/MzU2IzE=/nama-ibukota-kabupaten-kota-di-provinsi-riau.html

BSSN, D. B. O. K. S. dan S. (2023). Laporan tahunan layanan honeynet tahun 2025.

Dhanya, D. (2025). Indonesia's BSSN records 3.64 billion cyberattacks in first half of 2025. *En.Tempo.Co*. https://en.tempo.co/read/2037469/indonesias-bssn-records-3-64-billion-cyberattacks-in-first-half-of-2025

Fadli Mutaqin, M., & Ferdiansyah, D. (2022). Identifikasi kerentanan terhadap serangan slot backdoor pada website di Indonesia dengan menggunakan metode OSINT. *Jurnal Pasundan Informatika, 1*(2), 2986–5360. https://doi.org/10.29322/IJSRP.X.X.2018.pXXXX

Indonesia, C. (2023). BSSN ungkap Riau paling sering kena serangan siber, ada apa? *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20230613143456-192-961224/bssn-ungkap-riau-paling-sering-kena-serangan-siber-ada-apa

Nurhidayat, T., Oktavianto, D., Susila, W., Trianto, N., Firmasyah, I., Shofiyuddin, F. M., Permatasari, N., Mahardhika, S., Nuha, M. A. Ulin, Novazrianto, D., & Saputra, A. A. (2024). *Kajian ketahanan siber manajemen kerentanan*. Politeknik Siber dan Sandi Negara Press.

Nurseno, M., Aditiawarman, U., Al Qodri Maarif, H., & Mantoro, T. (2024). Detecting hidden illegal online gambling on .go.id domains using web scraping algorithms. *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer, 23*(2), 365–378. https://doi.org/10.30812/matrik.v23i2.3824

PENGGUNAAN NAMA DOMAIN Go.Id UNTUK SITUS WEB RESMI PEMERINTAHAN PUSAT DAN DAERAH (2006).

Projectdiscovery.io. (2023). An in-depth guide to subfinder: Beginner to advanced. *Projectdiscovery.io*. https://projectdiscovery.io/blog/do-you-really-know-subfinder-an-in-depth-guide-to-all-features-of-subfinder-beginner-to-advanced#introduction-to-subfinder

Projectdiscovery.io. (2025). *Subfinder*. https://github.com/projectdiscovery/subfinder

Q Fadlan. (2025). An evaluation of OSINT tools for external attack surface mapping. *Jurnal Teknologi Dan Manajemen Industri Terapan, 4*(3), 1195–1199. https://doi.org/10.55826/jtmit.v4i4.1415

Raharja, Y. (2024). *JIP (Jurnal Informatika Polinema) implementasi metode OSINT untuk mengidentifikasi serangan judi online pada website*. *JIP (Jurnal Informatika Polinema), 10*(3), 359–364.

Riau, D. K. I. dan S. (2021). *Grand design Riau digital provinsi Riau 2021-2025*. Diskominfotik Provinsi Riau.

The NIST Cybersecurity Framework (CSF) 2.0. (2024). https://doi.org/10.6028/NIST.CSWP.29

Utami, A. R. (2022). Pelatihan pembuatan website sebagai media promosi digital sepatu Mojo. *Jurnal Pengabdian Masyarakat Sabangka, 1*(04 SE-Articles), 104–110. https://doi.org/10.62668/sabangka.v1i04.245

Woncharso, E., Ahyar Muawwal, & Afifah. (2021). Penerapan search engine optimization (SEO) untuk meningkatkan pengunjung pada website SCLEAN. *KHARISMA Tech, 16*(2), 141–155. https://doi.org/10.55645/kharismatech.v16i2.139