ANALISIS STATUS KEAMANAN DOMAIN EMAIL APILOGY.ID MENGGUNAKAN DMARC (*DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE*)

LAPORAN SKRIPSI

REGINA PATRICIA THEYSER 1907421031

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

ANALISIS STATUS KEAMANAN DOMAIN EMAIL APILOGY.ID MENGGUNAKAN DMARC (*DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE*)

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik

REGINA PATRICIA THEYSER
1907421031

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2023

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	:	Regina Patricia Theyser
NIM	:	1907421031
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Status Keamanan Domain Email Apilogy.id Menggunakan DMARC (*Domain-Based Message Authentication, Reporting, and Conformance*)

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 24 Agustus 2023

Yang membuat pernyataan

Regina Patricia Theyser

NIM. 1907421031

LEMBAR PENGESAHAN

Skripsi diajukan oleh :
Nama .: Regina Patricia Theyser
NIM : 1907421031
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Status Keamanan Domain Email Apilogy.id menggunakan DMARC (Domain-Based Message Authentication, Reporting, and Conformance)
Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari ....Selasa., Tanggal ..22., Bulan.....Agustus....., Tahun 2023 dan dinyatakan LULUS.

Disahkan oleh

Pembimbing I : Defiana Arnaldy, S.Tp., M.Si.

Penguji I : Ayu Rosyida Zain, S.ST., M.T.

Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom.

Penguji III : Indra Hermawan, S.Kom., M.Kom

Mengetahui :
Jurusan Teknik Informatika dan Komputer
Ketua

Dr., Anita Hidayati , S.Kom., M.Kom.
NIP 197908032003122003

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan skripsi yang berisi tentang "**Analisis Status Keamanan Domain Email Apilogy.id menggunakan DMARC (*Domain-Based Message Authentication, Reporting, and Conformance*)**". Saran dan kritik yang sifatnya membangun begitu diharapkan oleh penyusun demi kesempurnaan dalam penulisan proposal. Dalam kesempatan ini, penulis mengucapkan banyak terima kasih kepada semua pihak yang telah membantu penulis menyelesaikan penyusunan skripsi di antaranya:

a. Ibu Dr. Anita Hidayati, S.Kom., M.Kom., selaku Ketua Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
b. Ibu Dr. Prihatin Oktaviasari, S.Si., M.Si. selaku Kepala Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
c. Bapak Defiana Arnaldy, S.Tp., M.Si., selaku dosen pembimbing yang telah membimbing penyusunan skripsi ini;
d. Pihak Telkom INS (*Digital Infrastructure and Security*) yang telah memberikan kepercayaan dan dukungan kepada penulis untuk melaksanakan skripsi;
e. Orang tua, adik, keluarga, sahabat, dan teman-teman yang senantiasa mendoakan dan memberikan dukungan secara moral dan material.

Akhir kata, diharapkan semoga semua pihak yang terlibat dan telah membantu mendapat balasan dan kebaikan. Semoga laporan skripsi yang diselesaikan membawa manfaat bagi pengembangan ilmu ke depannya.

Depok, 05 Juli 2023

Penulis

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama	:	Regina Patricia Theyser
NIM	:	1907421031
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

ANALISIS STATUS KEAMANAN DOMAIN EMAIL APILOGY.ID MENGGUNAKAN DMARC *(DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE)*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/ formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.. Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 24 Agustus 2023

Yang membuat pernyataan

Regina Patricia Theyser

NIM. 1907421031

Analisis Status Keamanan Domain Email Apilogy.id menggunakan DMARC

(*Domain-Based Message Authentication, Reporting, and Conformance*)

Abstrak

Email phishing merupakan salah satu kejahatan keamanan yang paling cepat berkembang dan merugikan bisnis maupun individu. Minimnya kesadaran dan pengetahuan seseorang untuk menjaga keamanan data sensitif dalam pesatnya perkembangan teknologi. Apilogy.id merupakan sebuah domain produk layanan baru PT Telkom Indonesia yang menyediakan layanan API (Application Programming Interface) kepada user. Untuk mencegah adanya penyalahgunaan serangan email spoofing yang mengatasnamakan domain email Apilogy.id, maka diterapkan metode DMARC (Domain-based Message Authentication, Reporting, and Conformance) yang merupakan metode autentikasi email untuk meningkatkan keamanan domain email publik, seperti Apilogy.id dan mampu melakukan monitoring status keamanan terhadap semua pesan yang terkirim ke domain email penerima dengan mengatasnamakan domain email Apilogy.id secara tidak resmi dengan menerapkan konfigurasi DMARC, DKIM, dan SPF yang diterapkan ke DNS Apilogy.id menggunakan tools DMARC Report. Penelitian ini dibentuk dari hasil analisis tiap tahapan, mulai dari perancangan, implementasi hingga analisis hasil pengujian pada domain yang dikonfigurasi DMARC dengan jenis kebijakan none, quarantine, dan reject secara bergantian. Kemudian diuji dengan mengirimkan email spoofing dari Apilogy.id menggunakan Caniphish dan Emkei's Fake Mailer ke 10 domain email penerima yang berbeda. Isi pesan email spoofing yang dikirimkan berisi tautan phishing yang dibuat menggunakan tools Socialfish dan Portmap.io. Penelitian bertujuan untuk mengetahui keberhasilan jenis kebijakan DMARC dalam mencegah pihak tidak bertanggung jawab mengirimkan pesan email mengatasnamakan domain email Apilogy.id secara tidak resmi. Hasil tingkat keakuratan pengiriman email spoofing dengan jenis skenario none (semua email masuk ke inbox penerima email) menggunakan Caniphish sebesar 80% dan Emkei's Fake Mailer sebesar 62%., tingkat keakuratan pengiriman email spoofing dengan jenis skenario quarantine (email tidak resmi masuk ke spam penerima email) menggunakan Caniphish sebesar 40% dan Emkei's Fake Mailer sebesar 70%, dan tingkat keakuratan pengiriman email spoofing dengan jenis skenario reject (email tidak resmi ditolak penerima email) menggunakan Caniphish sebesar 100% dan Emkei's Fake Mailer sebesar 96,67% berdasarkan hasil pengujian pada penelitian.

***Kata Kunci**: Apilogy.id, DMARC, Keamanan Email, Phishing, Spoofing.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi sekarang ini tidak hanya memberikan manfaat yang mempermudah segala aktivitas manusia. Namun, juga mendorong semakin banyaknya celah dan serangan keamanan karena kurangnya kesadaran seseorang dalam menjaga keamanan data. Dalam melakukan serangan keamanan terdapat beberapa tahapan yang harus dilalui oleh peretas. Langkah yang dilakukan sebelum melakukan serangan adalah mengumpulkan informasi (*Information Gathering*), memindai kerentanan (*Vulnerability Scanning*), kemudian melakukan eksploitasi (*Exploiting*) untuk menemukan titik lemah target berupa percobaan teknik serangan (Arnaldy & Perdana, 2019).

Berdasarkan data statistik *phishing* terbaru tahun 2023, *phishing* masih menjadi serangan keamanan yang paling umum dan berbahaya. Data resmi Indonesia Anti-Phishing Data Exchange (IDADX) dari Pengelola Nama Domain Internet Indonesia (PANDI) melaporkan bahwa tercatat sebanyak 26.675 serangan *phishing* yang menargetkan domain ".id" dan terdapat 99% domain *phishing* menggunakan protokol HTPPS selama kuartal pertama tahun 2023 (IDADX, 2023). Dari data tersebut, dapat dikatakan seiring dengan perkembangan teknologi setiap tahunnya, pelaku *phishing* akan terus menggunakan berbagai upaya untuk membuat target percaya bahwa tautan *phishing* tersebut aman untuk diakses.

Email merupakan standar layanan komunikasi yang banyak digunakan untuk bertukar informasi dengan mengirim dan menerima data, seperti *file* dokumen, gambar, surat dan lainnya (Riadi et al., 2022). Karena email berperan penting bagi antar individu maupun perusahaan, ini menjadikannya salah satu vektor serangan yang paling sering dilakukan. Pengiriman email *phishing* dengan memanfaatkan teknik *spoofing* domain adalah bentuk serangan umum yang digunakan oleh peretas melalui email (Shen et al., 2021). Serangan email *phishing* menjadi salah satu kejahatan dunia maya yang paling cepat berkembang di Internet yang dapat merugikan bisnis dan individu (Alhogail & Alsabih, 2021). Diperkirakan terdapat

3,4 miliar serangan ini dikirimkan melalui email spam setiap harinya (Griffiths, 2023). Di samping itu, sebanyak 67,5% karyawan perusahaan menjadi sasaran korban email *phishing* dengan tujuan mendapatkan informasi berharga perusahaan korban (Govender, 2023).

DMARC (*Domain-based Message Authentication, Reporting, and Conformance*) adalah standar metode autentikasi email yang dapat memberikan perlindungan terhadap domain organisasi dari penyalahgunaan, seperti serangan email *spoofing* terhadap domain email Apilogy.id yang berisi tautan *phishing*. Konfigurasi DMARC terdiri dari 3 yaitu *Sender Policy Framework* (SPF), *DomainKeys Identified Mail* (DKIM), dan DMARC itu sendiri yang terbukti memberikan keamanan yang lebih baik terhadap email penipuan. Metode ini telah terbukti efisien karena meminimalkan kompleksitas implementasi pengiriman pesan email sehingga memungkinkan hanya pengirim dan penerima yang sah yang dapat melewati pengiriman pesan tersebut (Nanaware et al., 2019).

Apilogy.id merupakan sebuah domain dari produk layanan baru PT Telkom Indonesia, yaitu Apilogy. Produk ini berfungsi untuk menghubungkan aplikasi *user* dengan ribuan produk dan layanan digital, serta memudahkan *user* terhubung dengan API (*Application Programming Interface*) Apilogy. Oleh karena itu, untuk mencegah terjadinya pemalsuan email yang mengatasnamakan domain email Apilogy.id secara tidak sah, maka perlu diterapkannya metode DMARC guna memantau status keamanan domain tersebut menggunakan *tools* DMARC *Report*. Oleh karena itu, pada penelitian ini diharapkan dapat menganalisis performa DMARC dalam mencegah dan melakukan *monitoring* domain email Apilogy.id dari pihak yang berusaha mengatasnamakan domain tersebut secara tidak resmi untuk melakukan serangan *spoofing* ke domain email korban.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, adapun beberapa masalah yang perlu dirumuskan adalah:

1. Bagaimana mengimplementasikan DMARC untuk *monitoring* status keamanan domain email Apilogy.id?

2. Bagaimana kinerja DMARC dalam mencegah domain email Apilogy.id dari pihak yang berusaha mengatasnamakan domain tersebut secara tidak resmi untuk melakukan serangan *spoofing* ke domain email korban?

1.3 Batasan Masalah

Adapun batasan masalah yang ditentukan dalam penelitian ini adalah sebagai berikut:

1. Fokus mengamankan domain email Apilogy.id sebagai domain layanan penyedia API (*Application Programming Interface*) di PT Telkom Indonesia.
2. *Tools* yang digunakan untuk *monitoring* status keamanan domain Apilogy.id adalah DMARC *Report*, sedangkan untuk skenario pengujian serangan email *spoofing* terhadap domain email Apilogy.id yang berisi tautan *phishing* menggunakan beberapa *tools* sebagai berikut.
   a.) Portmap.io dan Socialfish sebagai *tools* yang membuat tautan *phishing* pada isi pesan email *spoofing*.
   b.) Caniphish dan Emkei's *Fake Mailer* sebagai *tools* yang mengirimkan pesan email *spoofing* yang sudah disisipi tautan *phishing*.
3. Metode keamanan yang diimplementasikan pada domain email Apilogy.id adalah metode DMARC dengan tiga jenis kebijakan DMARC, yaitu *none*, *quarantine*, dan *reject* sebagai parameter yang dianalisis.
4. Skenario pengujian yang dilakukan adalah metode serangan pengiriman email *spoofing* terhadap domain email Apilogy.id yang berisi tautan *phishing* ke 10 domain email resmi. Dilakukan juga perbandingan dengan domain email yang tidak menerapkan metode DMARC, yaitu Apib**m.id. Pesan akan dikirimkan sebanyak lima kali ke setiap domain email target.
5. Hasil laporan *monitoring* yang ditampilkan *tools* DMARC *Report* berupa *Aggregate Report* yang menampilkan laporan, seperti total pesan yang dikirimkan, total pesan *compliant* (terdeteksi domain resmi), total pesan *non-compliant* (terdeteksi domain tidak resmi), total pesan dikarantina, dan total pesan ditolak yang semuanya mengatasnamakan domain email Apilogy.id

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengkonfigurasikan DMARC, DKIM, & SPF untuk dapat melakukan *monitoring* status keamanan domain email Apilogy.id menggunakan *tools* DMARC *Report*.
2. Menguji keberhasilan DMARC dalam mencegah dan melakukan *monitoring* serangan email *spoofing* terhadap domain email Apilogy.id.

1.4.2 Manfaat

Manfaat dari penelitian ini adalah sebagai berikut:

1. Dapat melakukan *monitoring* semua pesan email yang dikirimkan dengan mengatasnamakan domain email Apilogy.id berdasarkan jenis status keamanannya.
2. Dapat meningkatkan keamanan domain email Apilogy.id dengan mencegahnya dari serangan email *spoofing* ke alamat email target.

1.5 Sistematika Penulisan

Adapun metode atau urutan yang digunakan dalam menyelesaikan penyusunan penelitian ini adalah sebagai berikut:

1. BAB I PENDAHULUAN
   Pada bab ini, dilakukan identifikasi mengenai latar belakang dari permasalahan penting untuk diangkat sebagai topik penelitian skripsi.

2. BAB II TINJAUAN PUSTAKA
   Pada bab tinjauan pustaka dilakukan pengumpulan referensi yang berkaitan dengan penelitian, seperti jurnal, buku hingga *website* untuk mempelajari dan memahami landasan teori yang dijadikan sebagai acuan sehingga penelitian dapat menghasilkan data yang tepat, akurat, dan kredibel.

3. BAB III METODOLOGI PENELITIAN

   Bab metodologi penelitian menjelaskan terkait rancangan pendekatan penelitian, tahapan dalam menyelesaikan permasalahan, dan objek sasaran dari penelitian yang dikerjakan.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab hasil dan pembahasan berisi penjabaran mengenai analisis kebutuhan, perancangan, cara kerja, implementasi hingga pengujian keamanan pada sistem disertai dengan hasil analisis yang didapatkan.

5. BAB V PENUTUP

   Bab penutup berisi kesimpulan dan saran mengenai keseluruhan hasil analisis pengujian penelitian yang dilakukan dengan target awal dari perumusan masalah yang ingin dicapai. Adapun saran yang diberikan berdasarkan analisis perbaikan dari penelitian yang telah dilakukan untuk pengembangan topik penelitian selanjutnya.

BAB V
PENUTUP

5.1 Kesimpulan

Dalam meningkatkan keamanan domain email Apilogy.id dari serangan email *spoofing*, diterapkan metode DMARC (*Domain-Based Message Authentication, Reporting, and Comformance*) sesuai dengan jenis kebijakan *none*, *quarantine*, dan *reject* secara bergantian menggunakan *tools* DMARC *Report*. Hasil verifikasi DMARC didapatkan berdasarkan hasil autentikasi SPF (*Sender Policy Framework*) yang memastikan sumber pengirim berasal dari organisasi resmi dan DKIM (*DomainKeys Identified Mail*) yang mengecek bukti tanda tangan digital sumber pengirim sesuai dengan domain organisasi yang dicantumkan pada SPF.

Dari hasil pengujian pengiriman email *spoofing* berisi tautan *phishing* terhadap domain email Apilogy.id ke email publik lain dalam rentang 7 hari, didapatkan hasil tingkat keakuratan jenis kebijakan DMARC yang diterapkan dengan hasil kebijakan yang diterapkan oleh penerima email dari domain email Apilogy.id, antara lain:

- Tingkat keakuratan jenis kebijakan *none* yang diterapkan pada domain email Apilogy.id dalam mengatur kebijakan email penerima untuk menerima pesan email *spoofing* yang dikirimkan menggunakan Caniphish ke *inbox* lima alamat email penerima sebesar 80%, sedangkan untuk Emkei's *Fake Mailer* sebesar 62%. dari 10 alamat email penerima.
- Tingkat keakuratan jenis kebijakan *quarantine* dalam mengatur kebijakan email penerima dalam memindahkan pesan email *spoofing* ke folder spam sebesar 40% dari lima alamat email penerima untuk Caniphish dan 70% dari 10 alamat email penerima untuk Emkei's *Fake Mailer*.
- Tingkat keakuratan jenis kebijakan *reject* dalam mengatur kebijakan email penerima dalam menolak pesan email *spoofing* sebesar 100% dari lima alamat email penerima untuk Caniphish dan 96,67% dari 10 alamat email penerima untuk Emkei's *Fake Mailer*.

Berdasarkan hasil pengujian pada penelitian ini, dari ketiga jenis kebijakan DMARC, *reject* merupakan jenis kebijakan yang memiliki tingkat keakuratan dan kerentanan terkecil dalam penerimaan pesan email *spoofing*. Ini karena pesan yang berasal dari sumber pengirim yang terdeteksi tidak berhasil melewati autentikasi DKIM dan SPF otomatis ditolak sehingga memiliki tingkat kerentanannya pun paling rendah dibandingkan kedua jenis lainnya. Namun, dari hasil pengujian didapatkan bahwa *tools* DMARC *Report* memakan waktu yang lama karena membutuhkan waktu minimal 24 jam untuk menampilkan semua pesan yang masuk ke domain email Apilogy.id setelah dilakukan pengujian email *phishing*. Sehingga, dapat dikatakan jika *tools* ini tidak menampilkan semua pesan yang masuk secara *real time*.

5.1 Saran

1. Menggunakan *tools* serangan email *spoofing* yang lebih bervariasi untuk menguji performa metode DMARC yang telah diterapkan pada domain email Apilogy.id.

2. Menggunakan percobaan domain email yang memiliki fitur *Forensic Reports* agar dapat menganalisis jenis-jenis pesan email yang berbahaya yang mengatasnamakan domain email tersebut.

DAFTAR PUSTAKA

Alhogail, A., & Alsabih, A. (2021). Applying machine learning and natural language processing to detect phishing email. *Computers and Security*, *110*, 1–11. https://doi.org/10.1016/j.cose.2021.102414

Ali, G. A. (2020). Phishing Email: Could We Get Rid of It? A Review on Solutions to Combat Phishing Emails. *Advances in Intelligent Systems and Computing*, *1073*, 849–856. https://doi.org/10.1007/978-3-030-33582-3_80

Ananda, R. I., Fauziah, & Hayati, N. (2020). Keamanan Email Menggunakan Metode Pretty Good Privacy Dengan Algoritma Rsa. *Jurnal Ilmiah Informatika Komputer*, *25*(3), 213–224. https://doi.org/10.35760/ik.2020.v25i3.3118

Arnaldy, D., & Perdana, A. R. (2019). Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack. *2019 2nd International Conference of Computer and Informatics Engineering: Artificial Intelligence Roles in Industrial Revolution 4.0, IC2IE 2019*, 188–192. https://doi.org/10.1109/IC2IE47452.2019.8940872

Broadcom. (2023). *Intermittent SPF temperror results from sender authentication*. Broadcom. https://knowledge.broadcom.com/external/article/258012/intermitant-spf-temperror-results-from-s.html

CanIPhish. (2023). *Free Security Awareness Training | Phishing Simulation | CanIPhish*. CanIPhish. https://caniphish.com/

Chen, J., Paxson, V., & Jiang, J. (2020). Composition kills: A case study of email sender authentication. *Proceedings of the 29th USENIX Security Symposium*, 2183–2199.

DMARCReport.com. (2023). *What is a DMARC Forensic Report, and How Does*

it Differ from Aggregate Reports? | DMARC Report. https://dmarcreport.com/dmarc-forensic-report/

EASYDMARC. (2020, December 4). *SPF Authentication: SPF-all vs ~all | EasyDMARC*. https://easydmarc.com/blog/spf-authentication-spf-all-vs-all/

EASYDMARC. (2022, October 12). *What are DMARC Tags? | EasyDMARC*. https://easydmarc.com/blog/what-are-dmarc-tags-dmarc-tags-explained/

Faradilla. (2022). *Apa Itu Domain? Pengertian Domain dan Jenis-Jenisnya*. Hostinger. https://www.hostinger.co.id/tutorial/apa-itu-domain/

Google. (2023). *Add your DMARC record - Google Workspace Admin Help*. https://support.google.com/a/answer/2466563?hl=en

Govender, S. (2023). *50+ Statistik Spam & Phishing Email Yang Perlu Diketahui Pada Tahun 2023*. MarketSplash. https://marketsplash.com/id/statistik-spam/

Griffiths, C. (2023). *The Latest Phishing Statistics (updated March 2023) | AAG IT Support*. AAG. https://aag-it.com/the-latest-phishing-statistics/

IDADX. (2023). LAPORAN AKTIVITAS PHISHING DOMAIN .ID PERIODE Q1 2023. In *Indonesia Anti-Phishing Data Exchange (IDADX)*.

Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A comprehensive survey for intelligent spam email detection. *IEEE Access*, *7*, 168261–168295. https://doi.org/10.1109/ACCESS.2019.2954791

Konno, K., Kitagawa, N., & Yamai, N. (2020). False Positive Detection in Sender Domain Authentication by DMARC Report Analysis. *Proceedings of the 3rd International Conference on Information Science and Systems*, 38–42. https://doi.org/10.1145/3388176.3388217

Maroofi, S., Korczynski, M., Holzel, A., & Duda, A. (2021). Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis. *IEEE Transactions on Network and Service Management*, *18*(3), 3184–3196.

https://doi.org/10.1109/TNSM.2021.3065422

Marzuki, K., Hanif, N., & Hariyadi, I. P. (2022a). Application of Domain Keys Identified Mail, Sender Policy Framework, Anti-Spam, and Anti-Virus: The Analysis on Mail Servers. *International Journal of Electronics and Communications Systems*, *2*(2), 65–73. https://doi.org/10.24042/ijecs.v2i2.13543

Marzuki, K., Hanif, N., & Hariyadi, I. P. (2022b). Application of Domain Keys Identified Mail , Sender Policy Framework , Anti-Spam , and Anti-Virus : The Analysis on Mail Servers. *International Journal of Electronics and Communications System*, *2*(2), 65–73. https://doi.org/10.24042/ijecs.v2i2.13543

Microsoft. (2023). *Keamanan Outlook.com tingkat lanjut untuk pelanggan Microsoft 365 - Dukungan Microsoft*. Microsoft. https://support.microsoft.com/id-id/office/keamanan-outlook-com-tingkat-lanjut-untuk-pelanggan-microsoft-365-882d2243-eab9-4545-a58a-b36fee4a46e2

Mimecast. (2023). *DMARC Analyzer - Forensic DMARC Reports Explained*. https://community.mimecast.com/s/article/dmarc-analyzer-forensic-reports

mohdshariq. (2022, September 16). *Socialphish- Phishing Tool in Kali Linux - GeeksforGeeks*. GeeksforGeeks. https://www.geeksforgeeks.org/socialphish-phishing-tool-in-kali-linux/

Muralidharan, T., & Nissim, N. (2023). Improving malicious email detection through novel designated deep-learning architectures utilizing entire email. *Neural Networks*, *157*, 257–279. https://doi.org/10.1016/j.neunet.2022.09.002

MxToolBox. (2023, April 6). *Network Tools: DNS,IP,Email*. https://mxtoolbox.com/SuperTool.aspx?action=mx%3Aapilogy.id&run=toolpage

Nanaware, T., Mohite, P., & Patil, R. (2019). DMARCBox - Corporate Email

Security and Analytics using DMARC. *2019 IEEE 5th International Conference for Convergence in Technology, I2CT 2019*, 1–5. https://doi.org/10.1109/I2CT45611.2019.9033552

Ningtyas, S. (2020). *Apa itu Spoofing? Pahami Jenis-Jenis dan Cara Pencegahannya*. Niagarahoster. https://www.niagahoster.co.id/blog/spoofing-adalah/

Portmap.io. (2023). *Portmap.io - free port forwarding solution*. Portmap.Io . https://portmap.io/support

Reza. (2022). *Jenis-jenis Penetration Testing: Black Box, White Box, dan Gray Box - Fourtrezz*. FOURTREZZ. https://fourtrezz.co.id/articles/jenis-jenis-penetration-testing-black-box-white-box-dan-gray-box/

Riadi, I., Sunardi, & Nani, F. T. (2022). Analisis Forensik pada Email Menggunakan Metode National Institute of Standards Technology. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(2), 83–90. https://doi.org/10.14421/jiska.2022.7.2.83-90

Sakuraba, S., Yoda, M., Sei, Y., Tahara, Y., & Ohsuga, A. (2021). Improvement of Legitimate Mail Server Detection Method using Sender Authentication. *2021 IEEE/ACIS 19th International Conference on Software Engineering Research, Management and Applications, SERA 2021*, 10–14. https://doi.org/10.1109/SERA51205.2021.9509275

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*, *189*(2019), 19–28. https://doi.org/10.1016/j.procs.2021.05.077

Shen, K., Wang, C., Guo, M., Zheng, X., Lu, C., Liu, B., Zhao, Y., Hao, S., Duan, H., Pan, Q., & Yang, M. (2021). Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks. *Proceedings of the 30th USENIX Security Symposium*, 3201–3218.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, *4*(4), 225–230.

Symon, N. (2022). *What is an email domain and how to get one for your business?* Streak. https://www.streak.com/post/what-is-an-email-domain

Tatang, D., Zettl, F., & Holz, T. (2021). The evolution of DNS-based email authentication: measuring adoption and finding flaws. *ACM International Conference Proceeding Series*, 354–369. https://doi.org/10.1145/3471621.3471842

Umar, M. A. (2020). Comprehensive study of software testing: Categories, levels, techniques, and types. *TechRxiv*, 0–10. https://doi.org/10.36227/techrxiv.12578714.v2

Verma, P., Goyal, A., & Gigras, Y. (2020). Email phishing: text classification using natural language processing. *Computer Science and Information Technologies*, *1*(1), 1–12. https://doi.org/10.11591/csit.v1i1.p1-12

Wang, C., Shen, K., Guo, M., Zhao, Y., Zhang, M., Chen, J., Liu, B., Zheng, X., Duan, H., Lin, Y., & Pan, Q. (2022). A Large-scale and Longitudinal Measurement Study of DKIM Deployment. *Proceedings of the 31st USENIX Security Symposium, Security 2022*, 1185–1201.

Wirabattana, A. (2022). *Apa Itu SPF Record dan Bagaimana Cara Membuatnya?* Rumahweb. https://www.rumahweb.com/journal/apa-itu-spf-record-adalah/

LAMPIRAN

DAFTAR RIWAYAT HIDUP PENULIS

Penulis bernama Regina Patricia Theyser. Lahir di Jakarta, 22 Agustus 2001. Lulus dari SDN Cawang 10 Pagi Jakarta Timur tahun 2013, SMPN 281 Jakarta Timur tahun 2016, SMAN 51 Jakarta Timur tahun 2019. Saat ini sedang menempuh pendidikan Diploma IV Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

Lampiran 2 – Surat Pernyataan Izin Penelitian

Telkom Indonesia
the world in your hand

Nomor : Tel.110/PD 520/DBT-A2000000/2023

Jakarta, 16 Juni 2023

Kepada Yth.
Dr. Anita Hidayati, S.Kom., M.Kom.
Ketua Jurusan Teknik Informatika dan Komputer
Program Studi Teknik Multimedia dan Jaringan
Politeknik Negeri Jakarta

Lampiran : -
Perihal : **Surat Izin Penelitian Tugas Akhir - Regina Patricia Theyser**

Menunjuk surat Ketua Jurusan Teknik Informatika dan Komputer Program Studi Teknik Multimedia dan Jaringan Politeknik Negeri Jakarta Nomor: B.192/PL3.13/KM.07/2023 tanggal 28 Februari 2023 perihal Surat Izin Observasi atas nama:

Regina Patricia Theyser **NIM: 1907421031**

Dengan ini kami informasikan bahwa Mahasiswa tersebut dapat melaksanakan Kerja Praktek/ Penelitian mulai bulan **Maret s.d Agustus 2023** di TELKOM Direktorat Digital Business (DDB) — Divisi Digital Business & Technology (DBT) - **Digital Infrastructure and Security** dengan pembimbing **Sdr. Eko Permono Jati.**

Setiap Siswa yang akan melaksanakan Kerja Praktek/ Penelitian di TELKOM DDB wajib:

1. Mengisi surat pernyataan Kerja Praktek/ Penelitian (formulir disediakan) yang dilengkapi dengan pas Photo berwarna ukuran 4x6cm, dan diberi Materai Rp.10.000,-
2. Mematuhi ketentuan dan kebijakan yang berlaku di perusahaan.
3. Merahasiakan semua Informasi Rahasia yang dimiliki TELKOM (kategori Informasi tertulis dan diberi tanda "RAHASIA" dan/atau "TERBATAS" atau tanda yang sejenis; atau jika disampaikan secara lisan dan pada waktu pengungkapan pemilik informasi menyatakan bahwa informasi tersebut Rahasia.
4. Menyerahkan laporan Kerja Praktek/ Penelitian apabila telah selesai melaksanakan Kerja Praktek/Penelitian.

Kami informasikan pula bahwa pelaksanaan Kerja Praktek/ Penelitian dilakukan dengan mekanisme *Flexible Working Arrangement* (FWA), serta TELKOM DDB tidak menyediakan alat kerja (laptop), akomodasi, tunjangan transportasi maupun kompensasi lainnya untuk Siswa yang melaksanakan Kerja Praktek/ Penelitian di TELKOM DDB.

PT Telkom Indonesia, Tbk
Telkom Landmark Tower, 35th Floor
Jl. Gatot Subroto Kav 52, Jakarta - 12710

Direktorat Digital Business
Phone : +62 21 5225000
www.telkom.co.id

Apabila terjadi pembatalan terhadap kegiatan Kerja Praktek/ Penelitian ini, harap Saudara dapat memberitahukan kepada kami pada kesempatan pertama. Selanjutnya apabila membutuhkan informasi lebih lanjut mengenai Kerja Praktek/ Penelitian di TELKOM ODB, silakan menghubungi tim kami yaitu Sdri. Sendylenvi Regia (surel: s.regia@telkom.co.id dan nomor HP. 0812-217-1155) atau Sdri. Ina Marlina (surel: kerjapraktekddb@telkom.co.id dan nomor HP 0821-1634-1981).

Atas perhatian dan kerjasama Saudara kami ucapkan terima kasih.

Hormat Kami

Hepta Yuniarita
SM DIGITAL BUSINESS ENABLER DBT

Tembusan
1. Sdr. SM DIGITAL INFRASTRUCTURE & SECURITY DBT
2. Sdr. R.EKO PERMONO JATI , M.T.