Volume 15 Nomor 1 – April 2021

Info KriptO

Jurnal Ilmiah Keamanan Siber dan Kriptologi

ISSN 1978 - 7723

ISSN 1978-7723
April 2021
Hlm. 1 - 61
Nomor 1
Vol 15
INFO KRIPTO

- **Penilaian Kapabilitas Tata Kelola Keamanan Teknologi Informasi dan Rekomendasi Perbaikan Menggunakan COBIT 5**
  Ade Dwi Andayani, Obrina Candra Briliyant
- ***Security Assessment* pada Aplikasi *Mobile* Android XYZ dengan Mengacu pada Kerentanan OWASP *Mobile Top Ten* 2016**
  Candra Kurniawan, Nanang Trianto
- **Serangan Aljabar pada Algoritme S-IDEA dan Miniatur S-IDEA**
  Nadya Marta Matanggwan, Sa'aadah Sajjana Carita
- **Otomatisasi KARMA *Attack***
  Shandika Dianaji Santoso, M. Yusuf B. Setiadji
- **Desain PRNG Berbasis Fungsi *Hash* Menggunakan GIMLI**
  Galuh Dian Pradana, Nurul Qomariasih
- **Studi *Web Race Condition* Sebagai Acuan Pembuatan Modul Praktikum**
  Tio Hana Lolita B.L.T., Herman Kabetta
- **Serangan *Universal Forgery* pada Skema Fungsi *Hash* F_t, LightMAC_Plus, dan LightMAC_Plus2 Berbasis Algoritme DLBCA**
  Muhammad Ridwan, Andriani Adi Lestari

Pusat Penelitian dan Pengabdian Masyarakat
Politeknik Siber dan Sandi Negara (Poltek SSN)

ISSN 1978-7723

Info KriptO

Jurnal Ilmiah Keamanan Siber dan Kriptologi

Jurnal Info Kripto dipublikasikan oleh Pusat Penelitian dan Pengabdian Masyarakat Politeknik Siber dan Sandi Negara. Jurnal ini diterbitkan dari hasil penelitian dari berbagai bidang yang terkait dengan Keamanan Siber, Keamanan Informasi dan Kriptologi.

Penanggung Jawab
Nunil Pantjawati, B.Sc., M.E.
(Direktur Politeknik SSN)

Editor in Chief
Dr. Amiruddin, S.Kom., M.T.I.

Editor
Desi Marlena, S.T., M.T.
Arif Rahman Hakim, S.ST., M.Eng.
Nadia Paramita Retno Adiati, S.Si., M.Si.
R. Budiarto Hadiprakoso, MMSI.

Reviewer
Dr. Santi Indarjani, S.Si., MMSI.
Dr. Magfirawaty, S.Si., M.Si.
Dr. Bety Hayat Susanti, S.Si., M.E.
Setiyo Cahyono, S.Kom., M.T.
Dion Ogi, S.Pd., M.T.
Dr. Kiki Ariyanti Sugeng
Dr. Yohan Suryanto. S.T., M.T.
Dr. Charles Lim, B.Sc., M.Sc.

Sekretariat
Ray Novita Yasa, M.Si.
Rachmawati, A.Md.

Desain dan Layout
M. Febriansyah, A.Md.

SEKRETARIAT
Jurnal Info Kripto – Pusat Penelitian dan Pengabdian Masyarakat
Politeknik Siber dan Sandi Negara (Poltek SSN)
Telp (0251) 8541754, Fax (0251) 8541720
Email: infokripto@poltekssn.ac.id

PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa, karena atas limpahan rahmat dan karunia-Nya kami dapat menyelesaikan jurnal Info Kripto Volume 15 Nomor 1 Tahun 2021. Penyelesaian Jurnal Info Kripto ini merupakan hasil kerja sama berbagai pihak. Oleh karena itu, Kami selaku tim redaksi, mengucapkan terima kasih kepada penulis, editor dan semua pihak yang tidak dapat kami sebutkan satu persatu yang telah membantu penerbitan jurnal Info Kripto ini.

Jurnal Info Kripto merupakan salah satu sarana publikasi hasil penelitian civitas academica, khususnya yang berada di lingkungan Poltek SSN. Jurnal Info Kripto yang diterbitkan sebanyak tiga kali dalam setahun memuat hasil penelitian yang bertemakan kriptologi, keamanan informasi dan keamanan siber. Hadirnya Jurnal Info Kripto ini diharapkan dapat meningkatkan budaya penelitian yang kondusif dan komprehensif di lingkungan Poltek SSN.

Kami menyadari bahwa jurnal Info Kripto ini masih terdapat banyak kekurangan. Oleh karena itu, kami selalu terbuka terhadap kritik dan saran yang bersifat membangun untuk penerbitan jurnal Info Kripto yang lebih baik lagi pada edisi selanjutnya.

Bogor, April 2021

Editor in Chief

DAFTAR ISI

1. Penilaian Kapabilitas Tata Kelola Keamanan Teknologi Informasi dan Rekomendasi Perbaikan Menggunakan COBIT 5 1
2. Security Assessment pada Aplikasi *Mobile* Android XYZ dengan Mengacu pada Kerentanan OWASP *Mobile Top Ten* 2016..... 11
3. Serangan Aljabar pada Algoritme S-IDEA dan Miniatur S-IDEA 19
4. Otomatisasi KARMA *Attack*..... 27
5. Desain PRNG Berbasis Fungsi *Hash* Menggunakan GIMLI..... 35
6. Studi *Web Race Condition* Sebagai Acuan Pembuatan Modul Praktikum 45
7. Serangan *Universal Forgery* pada Skema Fungsi *Hash* F_t, LightMAC_Plus, dan LightMAC_Plus2 Berbasis Algoritme DLBCA..... 53