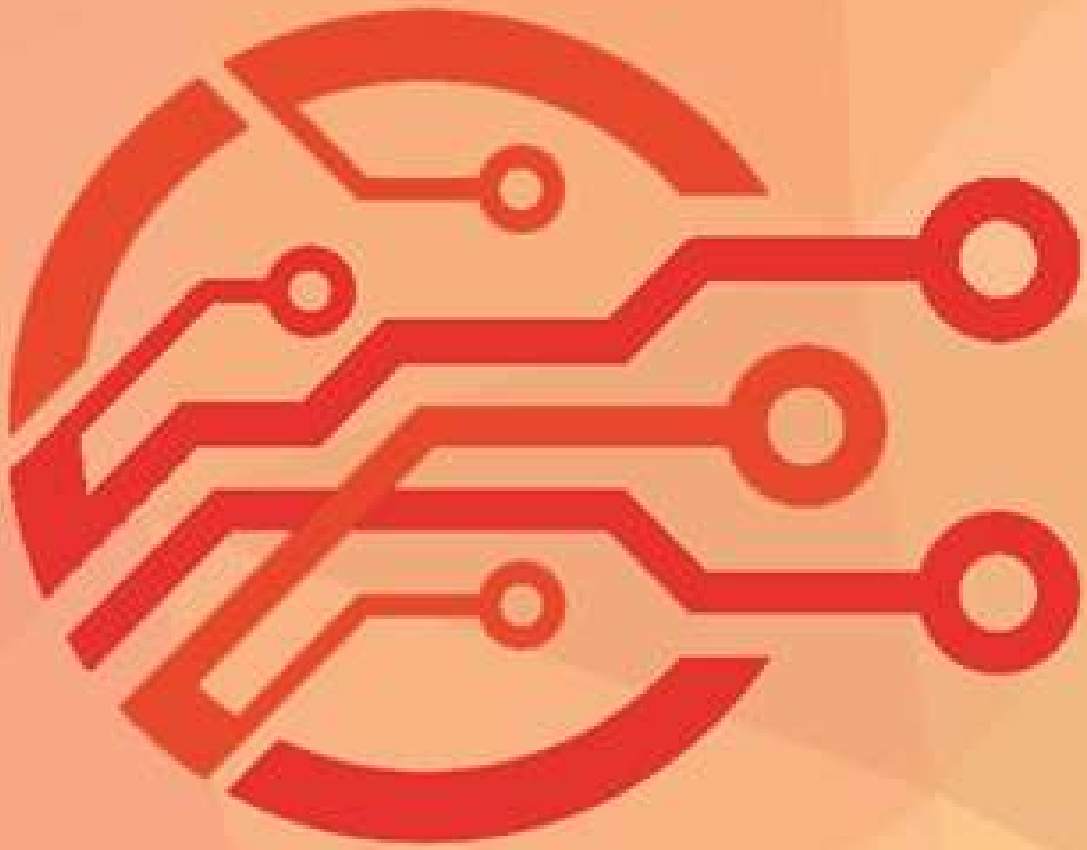
Smart Comp

Jurnal Orang Pintar Komputer



Politeknik Harapan Bersama Tegal

Jurnal SMART COMP

P-ISSN: 2089-676X
E-ISSN: 2549-0796

Smart Comp
Jurnalnya Orang Pintar Komputer
P-ISSN: 2089-676X
E-ISSN: 2549-0796

Reviewers

1. **Prof. Dr. Ir. Suhono Harso Supangkat, M.Eng.**
   Institution : Institut Teknologi Bandung
   Topics : Smart System Platform & Ecosystem, IT Architecture & Governance
   Profile : **Scopus** | **Google Scholar** | **Sinta**

2. **Prof. Dr. Kusrini, M.Kom.**
   Institution : Universitas AMIKOM Yogyakarta
   Topics : Artificial Intelligent, Decision Support System, Data Mining, Database
   Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

3. **Prof. Dr. Ema Utami, S.Si., M.Kom.**
   Institution : Universitas AMIKOM Yogyakarta
   Topics : Artificial Intelligent, Database, NLP, Data Science
   Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

4. **Prof. Dr. Raju Ganesh Sunder**
   Institution : Sharda University
   Topics : Energy Management, Sustainability, T&D IPTS, Reforms in Power, Power Management
   Profile : **Scopus** | **Google Scholar** | **ORCID**

5. **Dr. Dwi Prasetyo, Dipl.Inf., S.Kom., M.Si.**
   Institution : Universitas Nusa Cendana
   Topics : Retrival Information, GIS: Crime Mapping, E-Learning, M-Learning: Ubiquitos Learning
   Profile : **Sinta** | **ORCID**

6. **Dr. Henderi, M.Kom.**
   Institution : Universitas Raharja
   Topics : Sistem Informasi Akuntansi, E-Goverment
   Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

7. **Dr. Wing Wahyu Winarno, M.Sc.A.**
   Institution : STIE YKPN Yogyakarta
   Topics : Sistem Informasi Akuntansi, E-Goverment
   Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

8. **Dr. Usman Ependi, S.Kom., M.Kom.**
   Institution : Universitas Bina Darma
   Topics : Computer Science, Information System, Smart Cities
   Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

9. **Dr. Eng. Ir. Puput dani Prasetyo Adi, S.Kom., M.T.**
   Institution : Badan Riset dan Inovasi Nasional
   Topics : LPWA, LPWAN, IOT, Sensor Node Development
   Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

10. **Ir. Purwono, S.Kom., M.Kom.**
    Institution : Universitas Harapan Bangsa
    Topics : LPWA, LPWAN, IOT, Sensor Node Development
    Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

11. **Sumardi, M.Kom.**
    Institution : AMIK Jakarta Teknologi Cipta
    Topics : Sistem Informasi, Teknik Informatika

EDITORIAL TEAM
REVIEWERS
PEER REVIEW PROCESS
FOCUS AND SCOPE
AUTHOR GUIDELINE
PUBLICATION ETHICS
SCREENING PLAGIARISM
COPYRIGHT NOTICE
AUTHOR FEES
OPEN ACCESS POLICY
ONLINE SUBMISSION
JOURNAL HISTORY
REGISTRATION

SINTA SCORE & CERTIFICATE

SUPPORT & PARTNERSHIP

Profile : **Sinta**

12. **Rahmat Hidayat, M.Kom.**
Instiution : Politeknik Lamandau
Topics : Teknologi Informasi, Teknologi Rekayasa Komputer, Ilmu Komputer
Profile : **Google Scholar**

13. **Nabila Oper, M.Kom.**
Institution : Institut Teknologi dan Bisnis STIKOM Ambon
Topics : Teknik Informatika
Profile : **Google Scholar** | **Sinta**

14. **Darmanto, M.Kom.**
Institution : Politeknik Negeri Ketapang
Topics : Sistem Informasi
Profile : **Google Scholar** | **Sinta**

15. **Rosalina Yani Widiastuti, S.Kom., M.M.S.I.**
Institution : STIKOM Yos Sudarso
Topics : Technology, Information, System
Profile : **Google Scholar** | **Sinta**

16. **Arfan Haqiqi Sulasmoro, M.Kom.**
Institution : Politeknik Harapan Bersama
Topics : Data Mining, Algoritma, Pemrograman
Profile : **Google Scholar** | **Sinta** | **ORCID**

17. **Adhi Wibowo, S.Kom., M.M., MTI.**
Institution : STIKOM Yos Sudarso
Topics : Management, Information Technology, Information System
Profile : **Scopus** | **Google Scholar** | **Sinta**

18. **Diandra Chika Fransisca, S.Si., M.Sc.**
Institution : Institut Teknologi Telkom Purwokerto
Topics : Mathematics
Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

19. **Mutamassikin, M.Kom.**
Institution : UIN Sulthan Thaha Saifuddin Jambi
Topics : Technopreneur, Multimedia, Digital Marketing
Profile : **Scopus** | **Google Scholar** | **Sinta**

20. **Ida Afriliana, S.T., M.Kom.**
Institution : Politeknik Harapan Bersama
Topics : Database, Fuzzy Logic, Computer Vision
Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

21. **Purwanto, M.Kom.**
Institution : STMIK Tunas Bangsa Banjarnegara
Topics : Internet of Things, Data Science
Profile : **Google Scholar** | **Sinta**

22. **Eko Verianto, S.Kom., M.Cs.**
Institution : Universitas Cendekia Mitra Indonesia
Topics : Kecerdasan Buatan
Profile : **Google Scholar** | **Sinta**

23. **Annisa Fikria Shimbun, S.T., M.Kom.**
Institution : Universitas Cendekia Mitra Indonesia
Topics : SPK, Sistem Informasi
Profile : **Sinta**

24. **Oskar Ika Adi Nugroho, S.T., M.T.**
Institution : Sekolah Tinggi Ilmu Komputer Yos Sudarso
Topics : Human Pose Estimation, Human Action Recognition, Deep Learning, Machine Learning
Profile : **Google Scholar** | **Sinta**

25. **Nur Widjiyanti, M.Kom.**

Institution : Universitas Amikom Yogyakarta
Topics : Ilmu Komputer
Profile : **Google Scholar** | **Sinta**

26. Ibnu Hadi Purwanto, M.Kom.
Institution : Universitas Bina Darma
Topics : Sistem Informasi
Profile : **Scopus** | **Google Scholar** | **Sinta**

27. Ryan Putranda Kristianto, M.Kom.
Institution : Universitas Katolik Darma Cendekia
Topics : Software Engineering, Data Mining, Swarm Intelligence
Profile : **Scopus** | **Google Scholar** | **Sinta**

28. Jimi Asmara, M.Kom.
Institution : Universitas Nusa Cendana
Topics : Sistem Informasi
Profile : **Scopus** | **Google Scholar** | **Sinta**

29. Elfira Nureza Ardina, S.T., M.Tr.T.
Institution : Universitas Semarang
Topics : Teknologi Telekomunikasi, Teknik Telekomunikasi
Profile : **Scopus** | **Google Scholar** | **Sinta** | **ORCID**

30. Joko Dwi Santoso, M.Kom.
Institution : Universitas AMIKOM Yogyakarta
Topics : IoT, Cyber Security, Malware, Forensic Digital, Network Investigator
Profile : **Scopus** | **Google Scholar** | **Sinta**

31. Sudarmawan, M.T.
Institution : Universitas AMIKOM Yogyakarta
Topics : Teknologi Telekomunikasi, Teknik Telekomunikasi
Profile : **Scopus** | **Google Scholar** | **Sinta**

SMART COMP INDEXED OR REGISTERED BY

Smart Comp
Jurnalnya Orang Pintar Komputer
P-ISSN: 2089-676X
E-ISSN: 2549-0796

Editorial Team

Editor In Chief

Safar Dwi Kurniawan, M.Kom. (*Politeknik Harapan Bersama*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]

Managing Editor

Lukmanul Khakim, S.Kom., M.Tr.T. (*Politeknik Harapan Bersama*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]

Editorial Board

1. Dr. Dwi Prasetyo, Dipl.Inf., S.Kom., M.Si. (*Universitas Nusa Cendana*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]
2. Oman Somantri, M.Kom. (*Politeknik Negeri Cilacap*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]
3. Arif Rakhman, S.E., S.Pd., M.Kom. (*Politeknik Harapan Bersama*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]
4. Very Kurnia Bakti, M.Kom. (*Politeknik Harapan Bersama*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]
5. Eko Budihartono, S.T., M.Kom. (*Politeknik Harapan Bersama*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]
6. Miftakhul Huda, M.Kom. (*Politeknik Harapan Bersama*) [**Scopus** | **Google Scholar** | **Sinta**]
7. Marike Amelda Silvia Kondoj, M.T. (*Politeknik Negeri Manado*) [**Scopus** | **Google Scholar** | **Sinta** | **ORCID**]

SMART COMP INDEXED OR REGISTERED BY

Google Scholar · sinta Science and Technology Index · GARUDA Garba Rujukan Digital · Crossref · indonesia OneSearch · PKP|INDEX Public Knowledge Project · BASE · Dimensions · ISSN International Standard Serial Number International Centre · Index Copernicus International · DRJI Directory of Research Journal Indexing · Scilit Scientific Literature · IPIndexing Indexing Portal · OCLC WorldCat · Boston University

EDITORIAL TEAM
REVIEWERS
PEER REVIEW PROCESS
FOCUS AND SCOPE
AUTHOR GUIDELINE
PUBLICATION ETHICS
SCREENING PLAGIARISM
COPYRIGHT NOTICE
AUTHOR FEES
OPEN ACCESS POLICY
ONLINE SUBMISSION
JOURNAL HISTORY
REGISTRATION

SINTA SCORE & CERTIFICATE

S4 sinta Science and Technology Index

SUPPORT & PARTNERSHIP

MENDELEY · turnitin · RELAWAN JURNAL INDONESIA

ARTICLE TEMPLATES

USER

Username

Password

Remember me

Login

NOTIFICATIONS

- View
- Subscribe

LANGUAGE

Select Language

English

Submit

INFORMATION

- For Readers
- For Authors
- For Librarians

JOURNAL CONTENT

Search

Search Scope

All

Search

Browse

- By Issue
- By Author
- By Title
- Other Journals
- Categories

Smart Comp
Jurnalnya Orang Pintar Komputer
P-ISSN: 2089-676X
E-ISSN: 2549-0796

Vol 12, No 4 (2023)

Smart Comp: Jurnalnya Orang Pintar Komputer

Table of Contents

Articles

EDITORIAL TEAM
REVIEWERS
PEER REVIEW PROCESS
FOCUS AND SCOPE
AUTHOR GUIDELINE
PUBLICATION ETHICS
SCREENING PLAGIARISM
COPYRIGHT NOTICE
AUTHOR FEES
OPEN ACCESS POLICY
ONLINE SUBMISSION
JOURNAL HISTORY
REGISTRATION

SINTA SCORE & CERTIFICATE

SUPPORT & PARTNERSHIP

SMART COMP INDEXED OR REGISTERED BY

View My Stats

Analisis Keamanan Protokol Komunikasi *Message Queuing Telemetry Transport* (Studi Kasus Smart Greenhouse)

Andy Victor Pakpahan*[1], Mochamad Cory Sakti Triwangsa[2], Hanif Fakhrurroja[3]
[1,2,3]Teknik Informatika, Teknologi Informasi dan Digital, Institut Digital Ekonomi LPKIA
E-mail: *[1]**abang@lpkia.ac.id**, [2]mochamadcory.if03@gmail.com, [3]hani002@lipi.go.id

Abstrak

Masalah keamanan pada perangkat IoT menjadi isu yang menjadi kekhawatiran pengguna. Perangkat IoT yang memiliki pemrosesan yang terbatas menjadikan perangkat ini memiliki celah keamanan. Perangkat IoT kemudian menjadi sasaran oleh penyerang untuk mengambil data-data penggunanya. Perangkat IoT yang dianalisis keamanannya adalah Smart Greenhouse. Untuk menganalisis keamanan pada Smart Greenhouse menggunakan metode penetration testing dimana terhadap tahap Reconnaissance maka perlunya penggambaran sistem yang sedang berjalan dan berdasarkan sistem yang berjalan akan dicari celah berdasarkan studi literatur yang dilakukan. lalu potensi celah dicoba diimplementasikan di Smart Greenhouse dan dibandingkan dengan protokol komunikasi MQTTS yang dianggap lebih aman Kemudian pada tahap Scanning dilakukan dengan mencari informasi seperti IP, MAC dan port pada jaringan. Tahap ketiga adalah Exploitation melakukan penetrasi menggunakan teknik sniffling, Sniffling yang digunakan adalah ARP Poisoning, pada tahap Maintaining Access dilakukan MITM Attack kemudian ditemukan celah keamanan pada bagian protokol komunikasi MQTT yang digunakan, hal yang sama dilakukan pada MQTTS sebagai pembanding. Hasil implementasi tersebut ditemukan bahwa data yang dikirim melalui protokol MQTT dapat dibaca oleh penyerang dengan melakukan ARP Poisoning dan MITM Attack dapat memodifikasi packet data sehingga packet tidak sampai ke tujuan sedangkan pada protokol MQTTS ARP Poisoning dapat dilakukan namun data terenkripsi sehingga MITM Attack tidak dapat dilakukan.

.

Kata Kunci*— Analisis, Keamanan Protokol, MQTT, Smart Greenhouse, ARP Poisoning*

1. PENDAHULUAN

Smart Greenhouse adalah perangkat yang dikembangkan oleh PT. KREASI REKAYASA INDONESIA (KIREI), perangkat ini bertujuan untuk memberikan nutrisi pada tanaman dengan memeriksa kondisi tanah. Pengguna perangkat dapat memudahkan dalam me monitoring pertanian mereka tanpa harus mengawasi setiap saat dan memudahkan dalam pemberian nutrisi pada tanaman. Perangkat ini bekerja dengan cara mendapatkan data dari sensor tanah lalu memproses nya dengan algoritma sehingga menghasilkan keputusan bagi *actuator* untuk memberikan nutrisi yang sesuai, serta pengguna dapat menyalakan dan mematikan *actuator* seperti lampu pemanas untuk menjaga suhu dan kelembapan tanaman.

Masalah keamanan pada perangkat *IoT* menjadi isu yang menjadi kekhawatiran pengguna. Terdapat batasan keamanan yang telah diidentifikasi di perangkat *IoT* karena keterbatasan, daya, memori, dan kapasitas pemrosesan[1]. Keamanan yang dimaksudkan ialah keamanan pada aliran pengiriman data antara *microcontroller* dengan *cloud.* Keterbatasan tersebut yang menyebabkan perangkat *IoT* tidak memiliki keamanan yang memadai. Padahal kelemahan keamanan dapat berakibat fatal pada pemakainya maupun pengembang, seperti yang terjadi pada tokopedia yang mengalami kebocoran data dan harus didenda sebesar 100 miliar rupiah oleh Komunitas Konsumen Indonesia (KKI) pada tahun 2019 [2].

Pada *Smart Greenhouse* jika tidak diterapkan keamanan yang memadai maka perangkat tidak bekerja seperti semestinya. Misalnya ketika data sensor yang diambil tanah diubah maka kegiatan monitoring tidak akan berguna karena tidak menggambarkan keadaan aslinya hal ini juga akan mempengaruhi keputusan pengguna perangkat *IoT* yang ingin menyalakan aktuator melalui *website.*

Pengiriman data dari *microcontroller* ke *cloud* menggunakan protokol komunikasi. Protokol komunikasi yang digunakan oleh PT. KIREI yaitu *Message Queuing Telemetry Transport (MQTT)*. Berdasarkan jurnal penelitian [3] menyatakan protokol *MQTT* memiliki celah keamanan yang dapat digunakan untuk merusak data.

Berdasarkan permasalahan diatas, akan dilakukan analisis celah keamanan pada *MQTT* yang telah dipaparkan dengan membandingkannya dengan protokol lain

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam menganalisis protokol keamanan *MQTT* yang digunakan.

2.1. Studi Literatur

Studi Literatur (*literature review*) yaitu riset yang digunakan oleh peneliti dengan menghimpunkan sejumlah buku, jurnal, dan sumber kredibel lainnya yang berkaitan dengan masalah dan tujuan penelitian. Cara ini dilakukan dengan maksud untuk mengemukakan berbagai teori-teori yang signifikan dengan permasalahan yang sedang di observasi sebagai bahan sanad dalam pembahasan hasil penelitian[4].

2.2. Wawancara

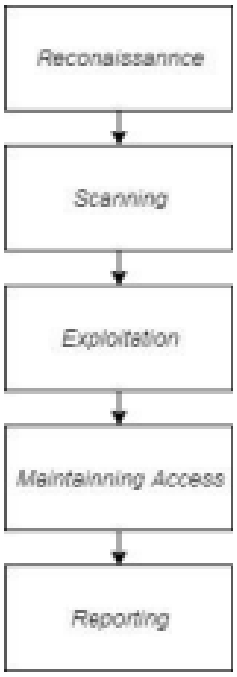
Perangkat wawancara digunakan dalam penelitian kualitatif karena dapat menyingkap informasi lintas waktu seperti waktu lampau, waktu sekarang, maupun waktu depan. Data yang dimanifestasikan dari wawancara bersifat terbuka, menyeluruh, dan tidak terbatas, sehingga sanggup membentuk informasi yang utuh dan komprehensif dalam mengungkap penelitian kualitatif [4].

2.3. Dokumentasi

Penelitian kualitatif tidak hanya menunjuk pada faktor sosial seperti yang bersua dalam kehidupan bermasyarakat, tetapi juga dapat melihata pada materi dalam bentuk arsip. Berbagai arsip itu seperti teks (berupa bacaan), rekaman audio, atau dalam bentuk audio visual. Segala ini biasa ditemui saat melaksanakan penelitian tentang naskah, karya sastra, dan seni pertunjukan [5].

2.4. Metode Penetration Testing

Penetration Testing (*Pentest*) merupakan aktivitas dimana seseorang membuktikan dengan mensimulasikan serangan terhadap sistem jaringan. Orang yang melaksanakan kegiatan ini dikenal sebagai penguji penetrasi [8]. *Penetration Testing* dapat diartikan sebagai sebuah cara yang legal dan formal untuk mendapatkan dan mengeksploitasi sistem komputer yang bertujuan untuk menciptakan sistem yang jauh lebih aman [10]. Tetapi pada beberapa persoalan, kerentanan yang didapat dari penguji penetrasi malah dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu sangat vital untuk memohonkan izin kepada pihak yang ingin di penguji penetrasi.



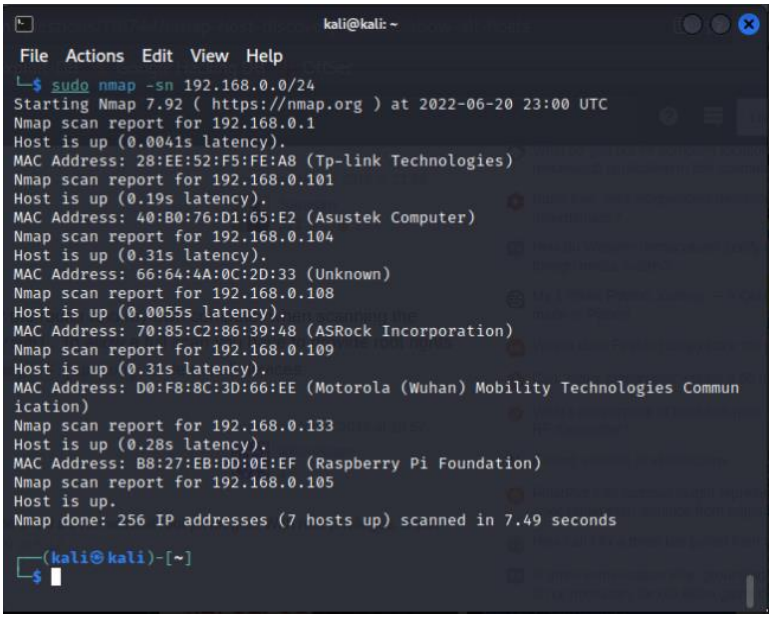
Gambar 1. Metode Penetration Testing

Berdasarkan Gambar 1, tingkatan *penetration testing* terdiri dari lima tahapan yakni mula-mula pada tahapan *Reconnaissance*, yaitu menetapkan medan pengujian dan metode pengujian yang akan dipakai pada topik penelitian. Kemudian pada tingkatan *Scanning* atau memindai sasaran menggunakan *tools* yang ada untuk mencari celah keamanan yang bisa digunakan untuk masuk ke dalam sistem. Kemudian pada tingkatan *Gaining Access* yaitu pengujian menerobos masuk dengan menggunakan teknik-teknik seperti *sniffing* dengan tujuan mengeksploitasi celah keamanan sistem, mencuri data, memantau lintas *traffic* jaringan yang berlangsung, dan monitoring kegiatan user pada objek yang diteliti. Kemudian pada tingkatan *Maintaining access*, yaitu apakah akses yang sudah didapatkan pada prosedur sebelumnya dapat ditutup sehingga keamanan pada sistem tetap aman. Dan tahap terakhir *Reporting* seperti pembuatan laporan dari rangkaian kegiatan yang sudah dilakukan

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

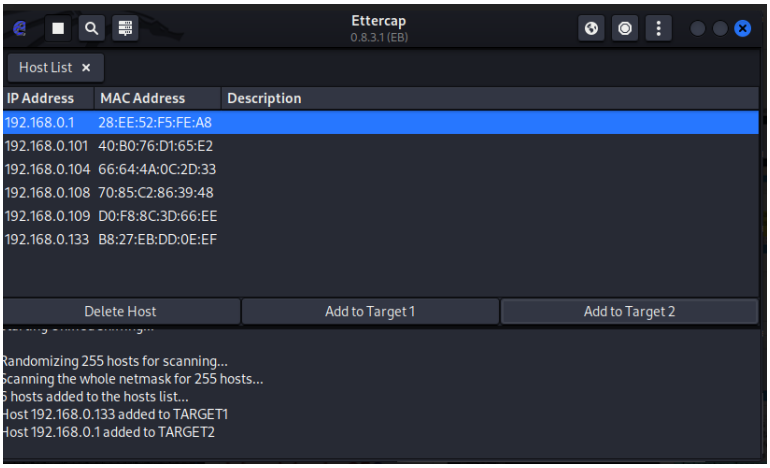
Berdasarkan analisis dan perancangan langkah pertama dalam *Penetration Testing* adalah *reconnaissance* yaitu mengumpulkan informasi yang diperlukan seperti mengumpulkan informasi perangkat *IoT* yang digunakan dan men scan *port* yang digunakan. Digunakan *tools* nmap pada kali linux yang terhubung dengan jaringan yang sama pada *target* seperti pada Gambar 2.



Gambar 2. Scanning IP and MAC address in the same network with nmap

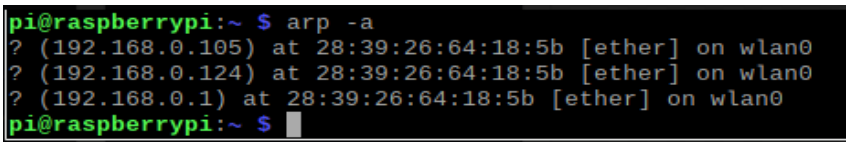
Berdasarkan Gambar 2, dengan menggunakan *nmap* proses pengumpulan informasi didapat bahwa *IP address* perangkat *IoT* yang terhubung pada jaringan yang sama memiliki *IP* 192.168.0.105 dengan *MAC Address* B8:27:EB:DD:0E:FF dan informasi router yang terhubung memiliki *IP address 192.168.0.1* dengan *MAC Address* 28:EE:52:F5:FE:A8. Informasi ini diperlukan untuk melakukan serangan *MITM* menggunakan Ettercap Filter.

Pada Ettercap lakukan *scanning* pada jaringan maka akan muncul *ARP table* seperti pada Gambar 3.



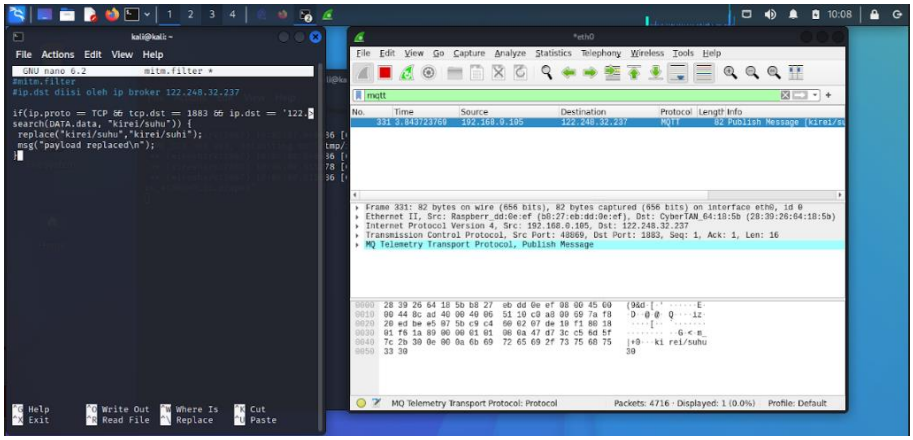
Gambar 3. list ARP table pada Ettercap

Berdasarkan Gambar 3, *IP* 192.168.0.133 dan *IP* 192.168.0.1 dipilih dan dimasukkan sebagai target 1 dan target 2. Setelah dijadikan target maka pilih Serangan *ARP Poisoning* maka serangan sedang berjalan. *ARP Poisoning* berjalan atau tidak dapat dideteksi pada raspberry dengan cara memasukkan perintah "arp –a" pada terminal maka pada IP yang berbeda memiliki *MAC Address* yang sama seperti pada Gambar 4,



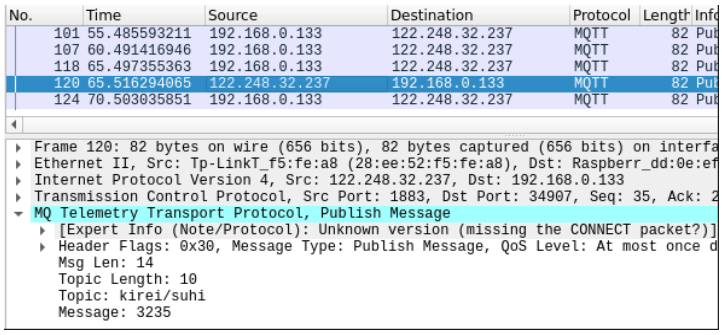
Gambar 4. ARP Poisoning berjalan

Setelah melakukan *ARP Poisoning* maka penyerang dapat melakukan *MITM*, untuk mengimplementasikan *MITM* digunakan Ettercap filter dan baris kode seperti pada Gambar 5.



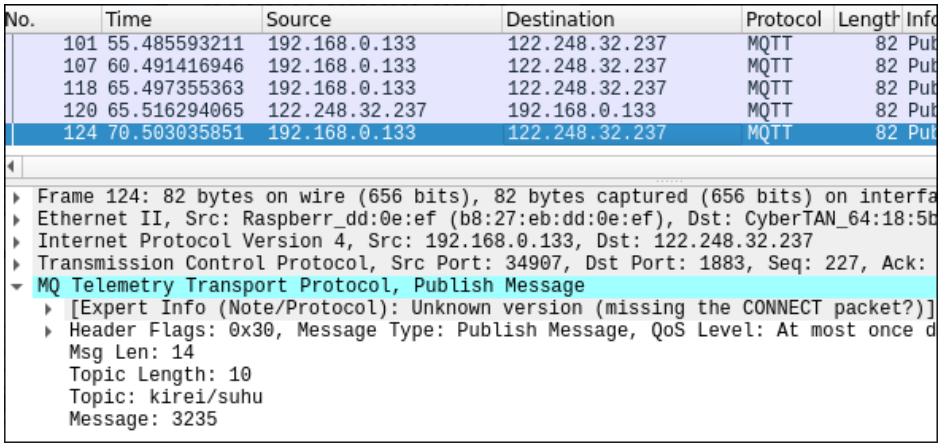
Gambar 5. memasukkan variabel hasil ARP Poisoning ke Ettercap Filter

Variabel ‘IP broker’ menggunakan hasil dari *ARP Poisoning* yang dapat mengetahui *IP broker* yang digunakan Smart Greenhouse, untuk mengganti data ketika proses transmisi data perlu diketahui data apa yang sedang dikirim, dengan menggunakan bantuan *tools* Wireshark dapat mendeteksi data yang dikirim melalui protokol *MQTT* berupa *plain text.* “kirei/suhu” adalah data yang dikirim ke server. Variabel tersebut dimasukkan kedalam baris kode gambar x dan variabel yang menjadi pengganti data adalah “kirei/suhi”. Setelah semua variabel dimasukkan. Maka kode program akan di-*compile* dan dijalankan oleh Ettercap Filter. Untuk mengetahui apakah serangan berhasil dilakukan maka akan diperiksa kembali transmisi data *MQTT* menggunakan Wireshark yang ditunjukkan pada Gambar 6 dan 7. Pada Gambar 6 transmisi data dari *server broker* ke perangkat *Raspberry* mengalami perbedaan data dengan yang ditunjukkan Pada Gambar 7



Gambar 6. MITM berhasil mengubah data integrity

Pada Gambar 6 transmisi data dari *server broker* ke perangkat *Raspberry* mengalami perbedaan data dengan yang ditunjukkan Pada Gambar 7.



Gambar 7. MITM berhasil mengubah data integrity

Berdasarkan analisis dan implementasi yang telah dilakukan didapat beberapa celah *MQTT* yang didapat yang ditunjukkan pada Tabel IV. 5

Tabel 1 Celah Keamanan MQTT

No	Nama Serangan	Status
1	*Search Engine* Shodan	Gagal
2	*ARP Poisoning*	Berhasil
3	*MITM Attack*	Berhasil

Sedangkan pada *MQTTS* yang didapat yang ditunjukkan pada Tabel 1.

Tabel 2 Celah Keamanan MQTTS

No	Nama Serangan	Status
1	*Search Engine* Shodan	Gagal
2	*ARP Poisoning*	Gagal
3	*MITM Attack*	Gagal

Berdasarkan studi literatur, hal ini terjadi karena pada protokol *MQTTS*, *MQTT* "dibungkus" oleh *TLS*, sehingga ketika pada proses transmisi data meskipun penyerang melakukan *sniffing*, penyerang tidak dapat menemukan informasi apapun dikarenakan data baru dapat dibaca ketika data telah sampai pada tujuan. Untuk kasus ini data telah sampai pada server *MQTT* dan server akan melakukan serangkaian tindakan untuk membukanya seperti memeriksa *certificate authentication, handshake, alert, changecipherspec,* dan *encryption*.

4. KESIMPULAN

Berdasarkan hasil analisis dan implementasi, protokol *MQTT* memiliki celah keamanan berupa serangan *ARP Poisoning* dan *MITM Attack.* Serangan tersebut tidak dapat dilakukan pada protokol *MQTTS.*

DAFTAR PUSTAKA

[1] Simon Kemp, 5 April 2022, Digital 2022 Indonesia :Internet use in Indonesia 2022, https://datareportal.com/reports/digital-2022 indonesia?rq=indonesia%202022.

[2] N. Rohman, R. Luviana Musyarofah, E. Utami, and S. Raharjo, "Natural Language Processing on Marketplace Product Review Sentiment Analysis," in 2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS), 2020, pp. 1–5, doi: 10.1109/ICORIS50180.2020.9320827.

[3] X. Wang, T. Zhou, X. Wang, and Y. Fang, "Harshness-aware sentiment mining framework for product review," Expert Systems with Applications, vol. 187, p. 115887, 2022, doi: https://doi.org/10.1016/j.eswa.2021.115887.

[4] J.-W. Bi, Y. Liu, and Z.-P. Fan, "Representing sentiment analysis results of online reviews using interval type-2 fuzzy numbers and its application to product ranking," Information Sciences, vol. 504, pp. 293–307, 2019, doi: https://doi.org/10.1016/j.ins.2019.07.025.

[5] Q. Wang, W. Zhang, J. Li, F. Mai, and Z. Ma, "Effect of online review sentiment on product sales: The moderating role of review credibility perception," Computers in Human Behavior, vol. 133, p. 107272, 2022, doi: https://doi.org/10.1016/j.chb.2022.107272.

[6] Kevin, V. et al. (2020) "Analisis Sentimen Transportasi Online Menggunakan Support Vector Machine Berbasis Particle Swarm Optimization (Online Transportation Sentiment Analysis Using Support Vector Machine Based on Particle Swarm Optimization)," Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 9(2), hal. 162–170FLEXChip Signal Processor (MC68175/D), Motorola, 1996.

[7] Y. Yennimar and R. Rizal, "Comparison of Machine Learning Classification Algorithms in Sentiment Analysis Product Review of North Padang Lawas Regency," SinkrOn, vol. 4, p. 268, 2019, doi: 10.33395/sinkron.v4i1.10416

[8] Sihombing, L., Hannie, H. dan Dermawan, B. (2021) "Sentimen Analisis Customer Review Produk Shopee Indonesia Menggunakan Algortima Naïve Bayes Classifier," Edumatic: Jurnal Pendidikan Informatika, 5, hal. 233–242. doi: 10.29408/edumatic.v5i2.4089

[9] M. T. Akter, M. Begum, and R. Mustafa, "Bengali Sentiment Analysis of E-commerce Product Reviews using K-Nearest Neighbors," in 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), 2021, pp. 40–44, doi: 10.1109/ICICT4SD50815.2021.9396910

[10] S. F. N. H. R. JAYADI, "Sentiment Analysis Of Indonesian E-Commerce Product Reviews Using Support Vector Machine Based Term Frequency Inverse Document," vol. 99, no. 17, pp. 4316–4325, 2022

POLITEKNIK HARAPAN BERSAMA
The True Vocational Campus

Nomor : 001.04/SMARTCOMP.PHB/VII/2023
Lampiran : -
Perihal : **Letter of Acceptance (LoA)**

Yth. Bapak/Ibu/Saudara:
Andy Victor Pakpahan, Muchamad Cory Sakti Triwangsa, dan Hanif Fakhrurroja.

Dengan Hormat,
Berdasarkan artikel saudara yang telah dikirimkan ke redaksi **Jurnal Smart Comp : Jurnalnya Orang Pintar Komputer**, Program Studi DIII Teknik Komputer, Politeknik Harapan Bersama dengan judul:

Analisis Keamanan Protokol Komunikasi Message Queuing Telemetry Transport (Studi Kasus Smart Greenhouse)

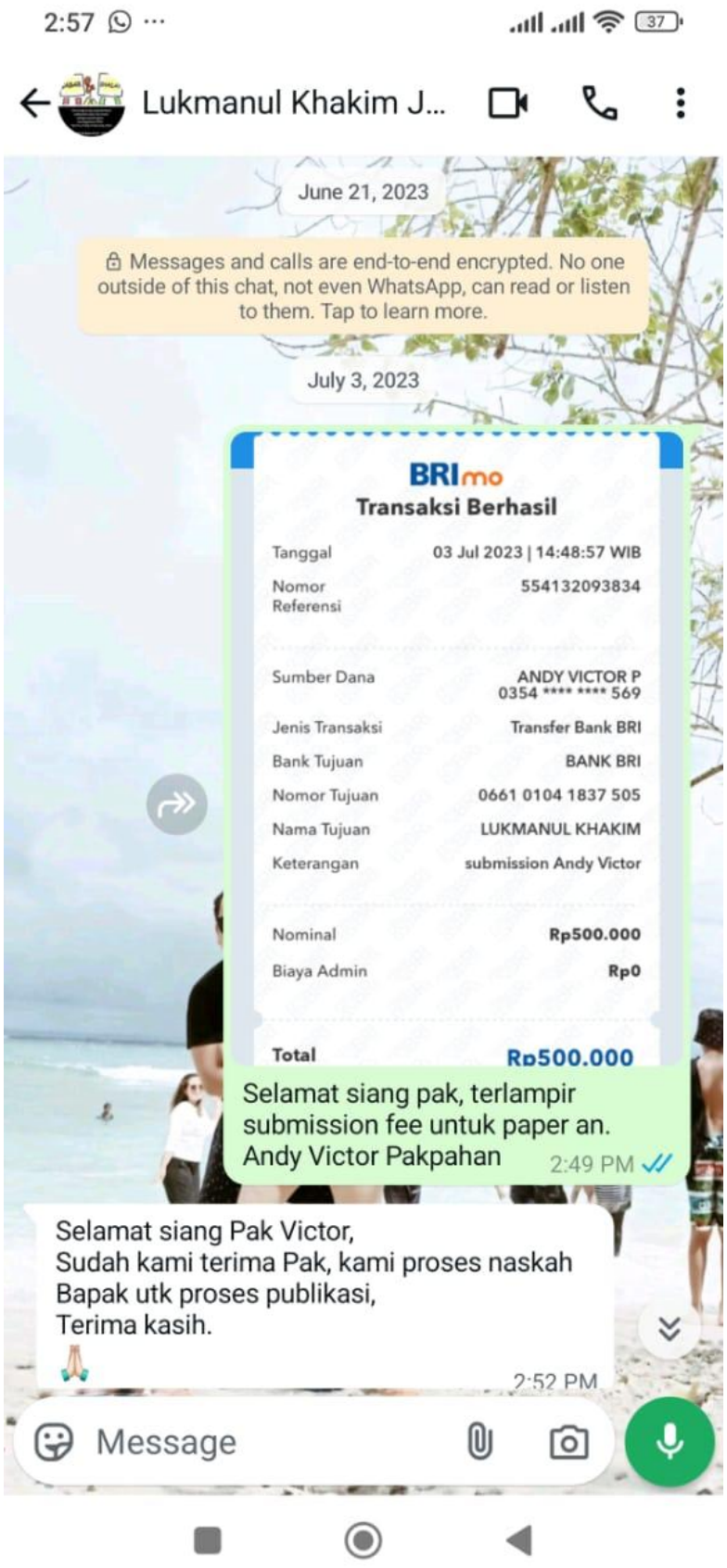
Bersamaan dengan ini kami sampaikan bahwa hasil penilaian dari mitra bestari dan dewan redaksi memutuskan bahwa artikel saudara telah layak dan diterima untuk diterbitkan di **Jurnal Smart Comp : Jurnalnya Orang Pintar Komputer,** di mana artikel saudara akan diterbitkan pada **Volume 12 Nomor 4, bulan Oktober 2023.**

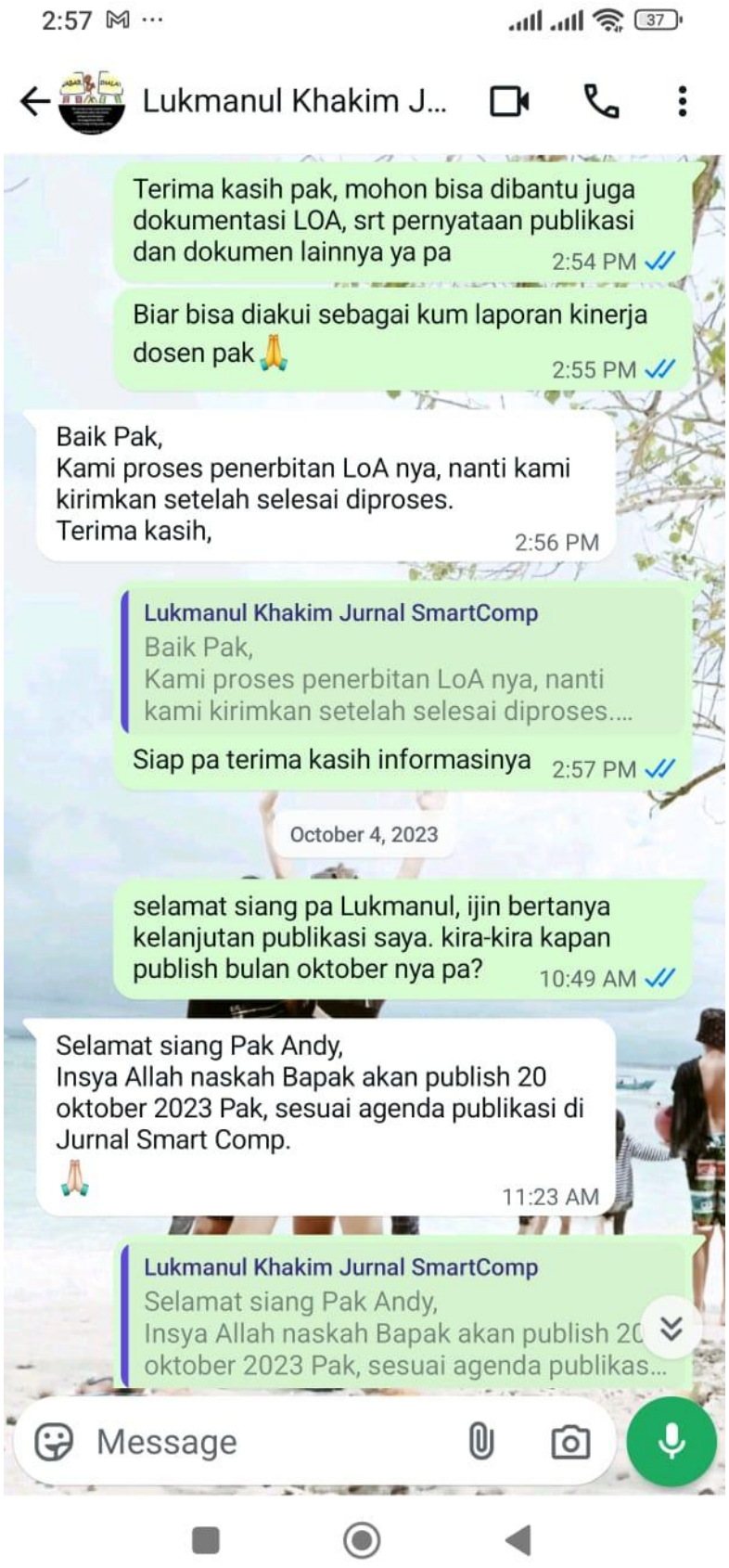
Demikian informasi ini kami sampaikan. Atas perhatian dan kerja samanya kami sampaikan terimakasih.

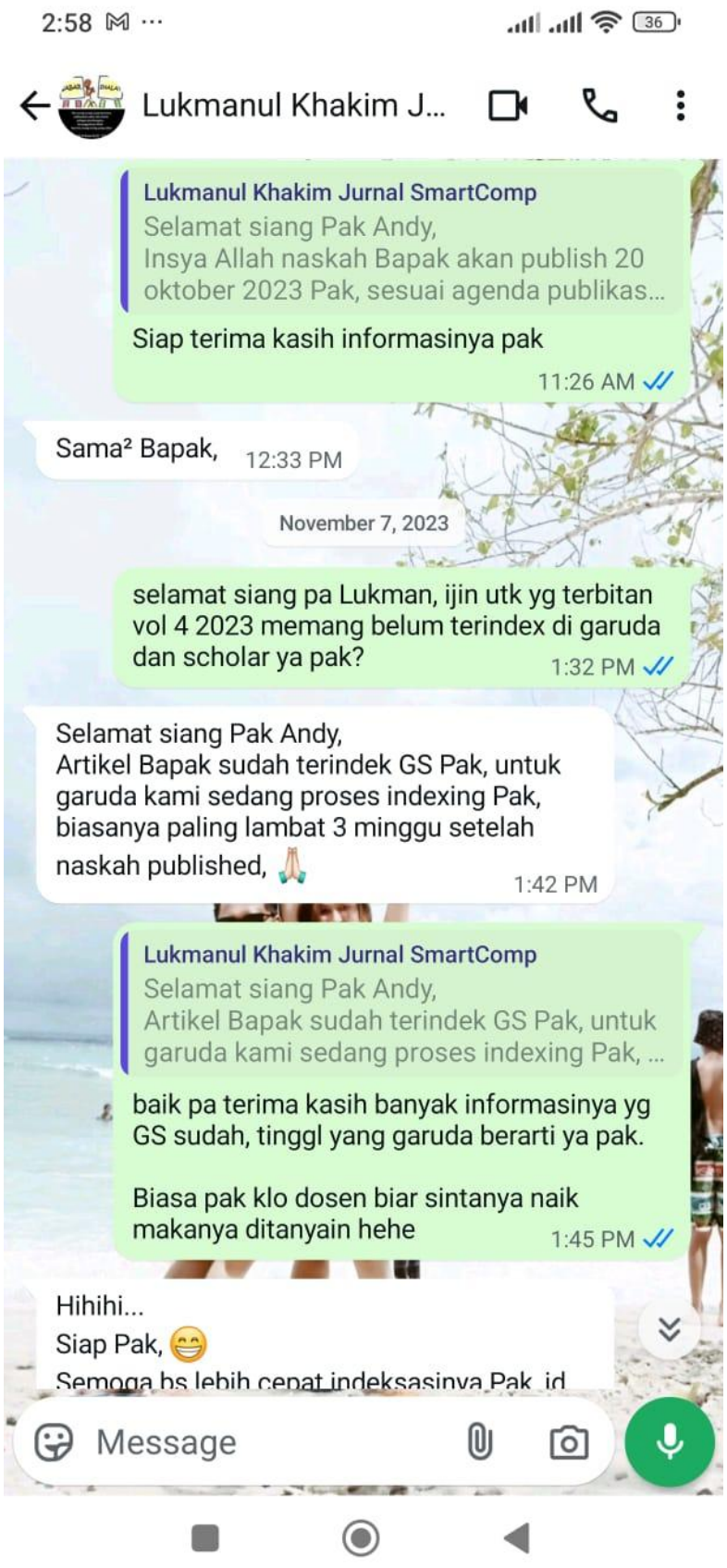
Tegal, 5 Juli 2023
Managing Editor,

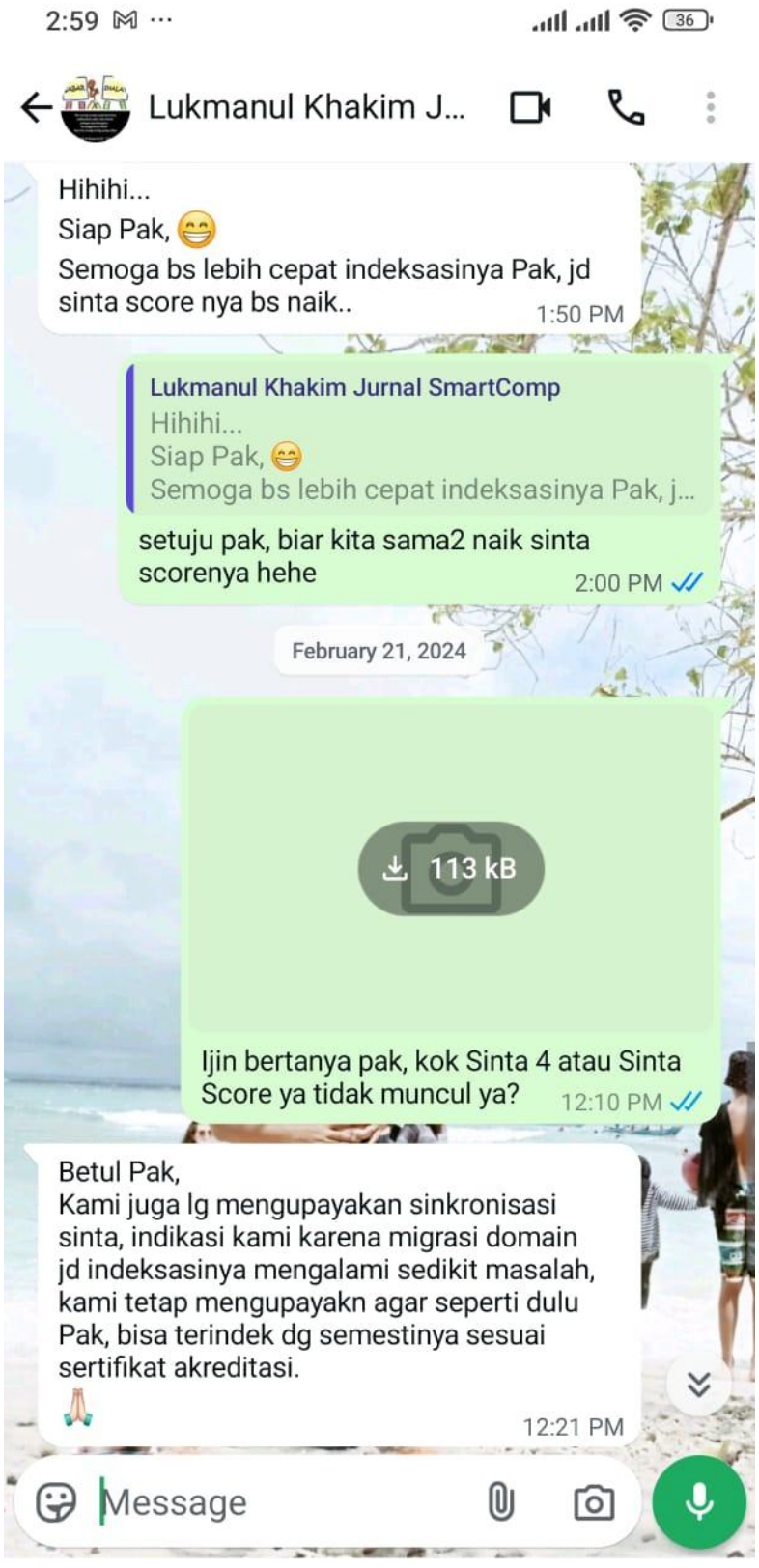
Lukmanul Khakim, S.Kom., M.Tr.T.
NIPY. 08.017.343

Jl. Mataram No. 9 Kota Tegal 52143, Jawa Tengah, Indonesia.
(0283)352000
p3m@poltektegal.ac.id
poltektegal.ac.id


2:57
Lukmanul Khakim J...
June 21, 2023
Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.
July 3, 2023
BRImo
Transaksi Berhasil
Tanggal 03 Jul 2023 | 14:48:57 WIB
Nomor Referensi 554132093834
Sumber Dana ANDY VICTOR P 0354 **** **** 569
Jenis Transaksi Transfer Bank BRI
Bank Tujuan BANK BRI
Nomor Tujuan 0661 0104 1837 505
Nama Tujuan LUKMANUL KHAKIM
Keterangan submission Andy Victor
Nominal Rp500.000
Biaya Admin Rp0
Total Rp500.000
Selamat siang pak, terlampir submission fee untuk paper an. Andy Victor Pakpahan 2:49 PM
Selamat siang Pak Victor,
Sudah kami terima Pak, kami proses naskah Bapak utk proses publikasi,
Terima kasih.
2:52 PM
Message


2:57
Lukmanul Khakim J...
Terima kasih pak, mohon bisa dibantu juga dokumentasi LOA, srt pernyataan publikasi dan dokumen lainnya ya pa
2:54 PM
Biar bisa diakui sebagai kum laporan kinerja dosen pak 🙏
2:55 PM
Baik Pak,
Kami proses penerbitan LoA nya, nanti kami kirimkan setelah selesai diproses.
Terima kasih,
2:56 PM
Lukmanul Khakim Jurnal SmartComp
Baik Pak,
Kami proses penerbitan LoA nya, nanti kami kirimkan setelah selesai diproses....
Siap pa terima kasih informasinya
2:57 PM
October 4, 2023
selamat siang pa Lukmanul, ijin bertanya kelanjutan publikasi saya. kira-kira kapan publish bulan oktober nya pa?
10:49 AM
Selamat siang Pak Andy,
Insya Allah naskah Bapak akan publish 20 oktober 2023 Pak, sesuai agenda publikasi di Jurnal Smart Comp.
🙏
11:23 AM
Lukmanul Khakim Jurnal SmartComp
Selamat siang Pak Andy,
Insya Allah naskah Bapak akan publish 20
oktober 2023 Pak, sesuai agenda publikas...
Message


2:58
Lukmanul Khakim J...
Lukmanul Khakim Jurnal SmartComp
Selamat siang Pak Andy,
Insya Allah naskah Bapak akan publish 20 oktober 2023 Pak, sesuai agenda publikas...
Siap terima kasih informasinya pak
11:26 AM
Sama² Bapak,
12:33 PM
November 7, 2023
selamat siang pa Lukman, ijin utk yg terbitan vol 4 2023 memang belum terindex di garuda dan scholar ya pak?
1:32 PM
Selamat siang Pak Andy,
Artikel Bapak sudah terindek GS Pak, untuk garuda kami sedang proses indexing Pak, biasanya paling lambat 3 minggu setelah naskah published,
1:42 PM
Lukmanul Khakim Jurnal SmartComp
Selamat siang Pak Andy,
Artikel Bapak sudah terindek GS Pak, untuk garuda kami sedang proses indexing Pak, ...
baik pa terima kasih banyak informasinya yg GS sudah, tinggl yang garuda berarti ya pak.
Biasa pak klo dosen biar sintanya naik makanya ditanyain hehe
1:45 PM
Hihihi...
Siap Pak,
Semoga bs lebih cepat indeksasinya Pak id
Message


2:59
Lukmanul Khakim J...
Hihihi...
Siap Pak,
Semoga bs lebih cepat indeksasinya Pak, jd sinta score nya bs naik..
1:50 PM
Lukmanul Khakim Jurnal SmartComp
Hihihi...
Siap Pak,
Semoga bs lebih cepat indeksasinya Pak, j...
setuju pak, biar kita sama2 naik sinta scorenya hehe
2:00 PM
February 21, 2024
113 kB
Ijin bertanya pak, kok Sinta 4 atau Sinta Score ya tidak muncul ya?
12:10 PM
Betul Pak,
Kami juga lg mengupayakan sinkronisasi sinta, indikasi kami karena migrasi domain jd indeksasinya mengalami sedikit masalah, kami tetap mengupayakn agar seperti dulu Pak, bisa terindek dg semestinya sesuai sertifikat akreditasi.
12:21 PM
Message

Andy Victor <abang@lpkia.ac.id>

Tagihan Biaya Penerbitan [Author Fees]

6 messages

Lukmanul Khakim <khakimthy@gmail.com> 21 June 2023 at 03:18
To: abang@lpkia.ac.id, Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id

Kepada Yth,
Author [Andy Victor Pakpahan, Mochamad Cory Sakti Triwangsa, Hanif Fakhrurroja]

Artikel anda dengan judul **"Analisis Keamanan Protokol Komunikasi Message Queuing Telemetry Transport (Studi Kasus Smart Greenhouse)",** telah selesai dilakukan review, dan sudah sesuai dengan scope jurnal Smart Comp. Selanjutnya untuk dapat dilakukan editing dan publikasi, silakan anda melakukan pembayaran sesuai dengan biaya yang tercantum pada Author Fees.

Pemabayaran dapat dilakukan dengan transfer ke nomor rekening sebagai berikut:
BRI : **066101041837505**
Nama : **Lukmanul Khakim**
Biaya Publikasi : **Rp.500.000,-**

Dimohon setelah selesai melakukan pembayaran dapat melakukan konfirmasi dan mengirimkan bukti transfer ke nomor **085642917672** (**Lukmanul Khakim**).
Atas perhatian dan kerja samanya, kami sampaikan terima kasih.

Managing Editor
Lukmanul Khakim
WA : 085642917672

*Note: Status **Accept Submission** akan didapatkan jika telah melakukan pembayaran sesuai dengan jumlah yang ditagihkan.*

==========
Regards,

Lukmanul Khakim
Phone/WA : 085642917672
==========

Andy Victor <abang@lpkia.ac.id> 21 June 2023 at 12:51
To: Lukmanul Khakim <khakimthy@gmail.com>
Cc: Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id

Siap terima kasih informasinya pak Lukmanul, ijin bertanya lebih lanjut maksimum pembayaran sampai kapan dan penerbitan utk bulan berapa?

Terima kasih
[Quoted text hidden]

Lukmanul Khakim <khakimthy@gmail.com> 21 June 2023 at 13:06
To: Andy Victor <abang@lpkia.ac.id>

Tenggat pembayaran sementara belum kami batasi Pak, hanya saja jika semakin lama pembayaran, maka waktu publish artikel Bapak juga akan semakin lama juga Pak.

[Quoted text hidden]

Mail Delivery Subsystem <mailer-daemon@googlemail.com> 22 June 2023 at 13:06
To: abang@lpkia.ac.id

Delivery incomplete

There was a temporary problem while delivering your message to **hani002@lipi.go.id**. Gmail will retry for 47 more hours. You'll be notified if the delivery fails permanently.

LEARN MORE

The response was:

```
The recipient server did not accept our requests to connect. Learn more at
https://support.google.com/mail/answer/7720 [mx1.lipi.go.id. 203.160.128.4: FAILED_PRECONDITION:
connect error (113): No route to host] [mx2.lipi.go.id. 203.160.128.5: FAILED_PRECONDITION:
connect error (113): No route to host] [mx3.lipi.go.id. 203.160.128.188: FAILED_PRECONDITION:
connect error (113): No route to host]
```

Final-Recipient: rfc822; hani002@lipi.go.id
Action: delayed
Status: 4.4.1
Diagnostic-Code: smtp; The recipient server did not accept our requests to connect. Learn more at
https://support.google.com/mail/answer/7720
[mx1.lipi.go.id. 203.160.128.4: FAILED_PRECONDITION: connect error (113): No route to host]
[mx2.lipi.go.id. 203.160.128.5: FAILED_PRECONDITION: connect error (113): No route to host]
[mx3.lipi.go.id. 203.160.128.188: FAILED_PRECONDITION: connect error (113): No route to host]
Last-Attempt-Date: Wed, 21 Jun 2023 23:06:41 -0700 (PDT)
Will-Retry-Until: Fri, 23 Jun 2023 22:51:33 -0700 (PDT)

---------- Forwarded message ----------
From: Andy Victor <abang@lpkia.ac.id>
To: Lukmanul Khakim <khakimthy@gmail.com>
Cc: Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id
Bcc:
Date: Wed, 21 Jun 2023 12:51:20 +0700
Subject: Re: Tagihan Biaya Penerbitan [Author Fees]
----- Message truncated -----

Mail Delivery Subsystem <mailer-daemon@googlemail.com> 23 June 2023 at 15:31
To: abang@lpkia.ac.id

Delivery incomplete

There was a temporary problem while delivering your message to **hani002@lipi.go.id**. Gmail will retry for 21 more hours. You'll be notified if the delivery fails permanently.

LEARN MORE

The response was:

```
The recipient server did not accept our requests to connect. Learn more at
https://support.google.com/mail/answer/7720 [mx1.lipi.go.id. 203.160.128.4: FAILED_PRECONDITION:
connect error (113): No route to host] [mx2.lipi.go.id. 203.160.128.5: FAILED_PRECONDITION:
connect error (113): No route to host] [mx3.lipi.go.id. 203.160.128.188: FAILED_PRECONDITION:
connect error (113): No route to host]
```

Final-Recipient: rfc822; hani002@lipi.go.id
Action: delayed
Status: 4.4.1
Diagnostic-Code: smtp; The recipient server did not accept our requests to connect. Learn more at
https://support.google.com/mail/answer/7720
[mx1.lipi.go.id. 203.160.128.4: FAILED_PRECONDITION: connect error (113): No route to host]
[mx2.lipi.go.id. 203.160.128.5: FAILED_PRECONDITION: connect error (113): No route to host]
[mx3.lipi.go.id. 203.160.128.188: FAILED_PRECONDITION: connect error (113): No route to host]
Last-Attempt-Date: Fri, 23 Jun 2023 01:31:05 -0700 (PDT)
Will-Retry-Until: Fri, 23 Jun 2023 22:51:33 -0700 (PDT)

---------- Forwarded message ----------
From: Andy Victor <abang@lpkia.ac.id>
To: Lukmanul Khakim <khakimthy@gmail.com>
Cc: Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id
Bcc:
Date: Wed, 21 Jun 2023 12:51:20 +0700
Subject: Re: Tagihan Biaya Penerbitan [Author Fees]
----- Message truncated -----

Mail Delivery Subsystem <mailer-daemon@googlemail.com> 24 June 2023 at 14:55
To: abang@lpkia.ac.id

Message not delivered

There was a problem delivering your message to **hani002@lipi.go.id**. See the technical details below or try resending in a few minutes.

LEARN MORE

The response was:

```
The recipient server did not accept our requests to connect. Learn more at
https://support.google.com/mail/answer/7720 [mx1.lipi.go.id. 203.160.128.4: FAILED_PRECONDITION:
connect error (113): No route to host] [mx2.lipi.go.id. 203.160.128.5: FAILED_PRECONDITION:
```

connect error (113): No route to host] [mx3.lipi.go.id. 203.160.128.188: FAILED_PRECONDITION:
connect error (113): No route to host]

Final-Recipient: rfc822; hani002@lipi.go.id
Action: failed
Status: 4.4.1
Diagnostic-Code: smtp; The recipient server did not accept our requests to connect. Learn more at
https://support.google.com/mail/answer/7720
[mx1.lipi.go.id. 203.160.128.4: FAILED_PRECONDITION: connect error (113): No route to host]
[mx2.lipi.go.id. 203.160.128.5: FAILED_PRECONDITION: connect error (113): No route to host]
[mx3.lipi.go.id. 203.160.128.188: FAILED_PRECONDITION: connect error (113): No route to host]
Last-Attempt-Date: Sat, 24 Jun 2023 00:55:45 -0700 (PDT)

---------- Forwarded message ----------
From: Andy Victor <abang@lpkia.ac.id>
To: Lukmanul Khakim <khakimthy@gmail.com>
Cc: Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id
Bcc:
Date: Wed, 21 Jun 2023 12:51:20 +0700
Subject: Re: Tagihan Biaya Penerbitan [Author Fees]
----- Message truncated -----

Andy Victor <abang@lpkia.ac.id>

Penerbitan Letter of Acceptance (LoA)

3 messages

Lukmanul Khakim <khakimthy@gmail.com> 5 July 2023 at 09:37
To: Andy Victor <abang@lpkia.ac.id>, Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id

Kepada Yth,
Author [Andy Victor Pakpahan, Muchamad Cory Sakti Triwangsa, dan Hanif Fakhrurroja]

Berikut kami kirimkan Letter of Acceptance (LoA) dari artikel yang anda kirimkan di Jurnal Smart Comp : Jurnalnya Orang Pintar Komputer.
Terima kasih

Managing Editor
Lukmanul Khakim

==========
Regards,

Lukmanul Khakim
Phone/WA : 085642917672
==========

[4681]-LoA-M Cory dkk.pdf
608K

Andy Victor <abang@lpkia.ac.id> 5 July 2023 at 10:04
To: Lukmanul Khakim <khakimthy@gmail.com>
Cc: Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com>, hani002@lipi.go.id

Terima kasih pak Lukmanul atas informasinya
[Quoted text hidden]

Lukmanul Khakim <khakimthy@gmail.com> 5 July 2023 at 10:07
To: Andy Victor <abang@lpkia.ac.id>

Sama² Bapak..
[Quoted text hidden]

Andy Victor <abang@lpkia.ac.id>

Fwd: Konfirmasi Penerbitan Artikel

1 message

Mochamad Cory Sakti Triwangsa <mochamadcory.if03@gmail.com> 21 June 2023 at 12:51
To: abang@lpkia.ac.id

---------- Forwarded message ---------
Dari: **Lukmanul Khakim** <khakimthy@gmail.com>
Date: Jum, 16 Jun 2023 pukul 17.54
Subject: Konfirmasi Penerbitan Artikel
To: <mochamadcory.if03@gmail.com>

Kepada Yth.
Author [Mochamad Cory Sakti Triwangsa]

Kami mengucapkan terima kasih dan mengapresiasi atas kepercayaan Anda untuk men-submit Naskah anda dengan judul **"Analisis Keamanan Protokol Komunikasi Message Queuing Telemetry Transport (Studi Kasus Smart Greenhouse)"** di Jurnal Smart Comp: Jurnalnya Orang Pintar Komputer, Naskah anda sudah sesuai dengan scope di jurnal kami, oleh karena itu kami membutuhkan konfirmasi anda jika artikel anda dimungkinkan dapat terbit pada tahun 2023, mohon berikan respon kesediaan anda melalui email ini atau WA ke 085642917672 (Lukmanul Khakim). Atas perhatian dan kerja samanya, kami sampaikan terima kasih.

Managing Editor
Lukmanul Khakim
WA: 085642917672
==========
Regards,

Lukmanul Khakim
Phone/WA : 085642917672
==========

cory v3

by Turnitin Turnitin

Submission date: 22-Nov-2022 12:32AM (UTC-0500)
Submission ID: 1961023126
File name: jurnal_skripsi2.pdf (435.48K)
Word count: 1903
Character count: 11933

Analisis Keamanan Protokol Komunikasi Message Queuing Telemetry Transport (Studi Kasus Smart Greenhouse)

Andy Viktor Pakpahan*[1], Mochamad Cory Sakti Triwangsa[2], Penulis ketiga[3]
[1,2,3]Teknik Informatika, Teknologi Informasi dan Digital, Institut Digital Ekonomi LPKIA
E-mail: *[1]abang@lpkia.ac.id, [2]mochamadcory.if03@gmail.com, [3]xxxx@xxxx.xxx

Abstrak

Masalah keamanan pada perangkat IoT menjadi isu yang menjadi kekhawatiran pengguna. Perangkat IoT yang memiliki pemrosesan yang terbatas menjadikan perangkat ini memiliki celah keamanan. Perangkat IoT kemudian menjadi sasaran oleh penyerang untuk mengambil data-data penggunanya. Perangkat IoT yang dianalisis keamanannya adalah Smart Greenhouse. Untuk menganalisis keamanan pada Smart Greenhouse menggunakan metode penetration testing dimana terhadap tahap Reconnaissance maka perlunya penggambaran sistem yang sedang berjalan dan berdasarkan sistem yang berjalan akan dicari celah berdasarkan studi literatur yang dilakukan. lalu potensi celah dicoba diimplementasikan di Smart Greenhouse dan dibandingkan dengan protokol komunikasi MQTTS yang dianggap lebih aman Kemudian pada tahap Scanning dilakukan dengan mencari informasi seperti IP, MAC dan port pada jaringan. Tahap ketiga adalah Exploitation melakukan penetrasi menggunakan teknik sniffling, Sniffling yang digunakan adalah ARP Poisoning, pada tahap Maintaining Access dilakukan MITM Attack kemudian ditemukan celah keamanan pada bagian protokol komunikasi MQTT yang digunakan, hal yang sama dilakukan pada MQTTS sebagai pembanding. Hasil implementasi tersebut ditemukan bahwa data yang dikirim melalui protokol MQTT dapat dibaca oleh penyerang dengan melakukan ARP Poisoning dan MITM Attack dapat memodifikasi packet data sehingga packet tidak sampai ke tujuan sedangkan pada protokol MQTTS ARP Poisoning dapat dilakukan namun data terenkripsi sehingga MITM Attack tidak dapat dilakukan.

.

Kata Kunci— *Analisis, Keamanan Protokol, MQTT, Smart Greenhouse, ARP Poisoning*

1. PENDAHULUAN

Smart Greenhouse adalah perangkat yang dikembangkan oleh PT. KREASI REKAYASA INDONESIA (KIREI), perangkat ini bertujuan untuk memberikan nutrisi pada tanaman dengan memeriksa kondisi tanah. Pengguna perangkat dapat memudahkan dalam me monitoring pertanian mereka tanpa harus mengawasi setiap saat dan memudahkan dalam pemberian nutrisi pada tanaman. Perangkat ini bekerja dengan cara mendapatkan data dari sensor tanah lalu memproses nya dengan algoritma sehingga menghasilkan keputusan bagi *actuator* untuk memberikan nutrisi yang sesuai, serta pengguna dapat menyalakan dan mematikan *actuator* seperti lampu pemanas untuk menjaga suhu dan kelembapan tanaman.

Masalah keamanan pada perangkat *IoT* menjadi isu yang menjadi kekhawatiran pengguna. Terdapat batasan keamanan yang telah diidentifikasi di perangkat *IoT* karena keterbatasan, daya, memori, dan kapasitas pemrosesan[1]. Keamanan yang dimaksudkan ialah keamanan pada aliran pengiriman data antara *microcontroller* dengan *cloud*. Keterbatasan tersebut yang menyebabkan perangkat *IoT* tidak memiliki keamanan yang memadai. Padahal kelemahan keamanan dapat berakibat fatal pada pemakainya maupun pengembang, seperti yang terjadi pada tokopedia yang

mengalami kebocoran data dan harus didenda sebesar 100 miliar rupiah oleh Komunitas Konsumen Indonesia (KKI) pada tahun 2019 [2].

Pada *Smart Greenhouse* jika tidak diterapkan keamanan yang memadai maka perangkat tidak bekerja seperti semestinya. Misalnya ketika data sensor yang diambil tanah diubah maka kegiatan monitoring tidak akan berguna karena tidak menggambarkan keadaan aslinya hal ini juga akan mempengaruhi keputusan pengguna perangkat *IoT* yang ingin menyalakan aktuator melalui *website*.

Pengiriman data dari *microcontroller* ke *cloud* menggunakan protokol komunikasi. Protokol komunikasi yang digunakan oleh PT. KIREI yaitu *Message Queuing Telemetry Transport (MQTT)*. Berdasarkan jurnal penelitian [3] menyatakan protokol *MQTT* memiliki celah keamanan yang dapat digunakan untuk merusak data.

Berdasarkan permasalahan diatas, akan dilakukan analisis celah keamanan pada *MQTT* yang telah dipaparkan dengan membandingkannya dengan protokol lain

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam menganalisis protokol keamanan *MQTT* yang digunakan.

2.1. Studi Literatur

Studi Literatur (*literature review*) yaitu riset yang digunakan oleh peneliti dengan menghimpunkan sejumlah buku, jurnal, dan sumber kredibel lainnya yang berkaitan dengan masalah dan tujuan penelitian. Cara ini dilakukan dengan maksud untuk mengemukakan berbagai teori-teori yang signifikan dengan permasalahan yang sedang di observasi sebagai bahan sanad dalam pembahasan hasil penelitian[4].

2.2. Wawancara

Perangkat wawancara digunakan dalam penelitian kualitatif karena dapat menyingkap informasi lintas waktu seperti waktu lampau, waktu sekarang, maupun waktu depan. Data yang dimanifestasikan dari wawancara bersifat terbuka, menyeluruh, dan tidak terbatas, sehingga sanggup membentuk informasi yang utuh dan komprehensif dalam mengungkap penelitian kualitatif [4].

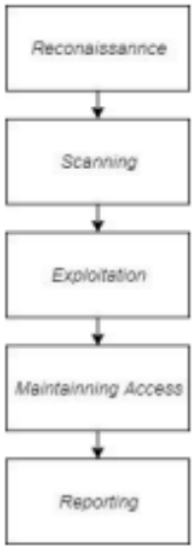
2.3. Dokumentasi

Penelitian kualitatif tidak hanya menunjuk pada faktor sosial seperti yang bersua dalam kehidupan bermasyarakat, tetapi juga dapat melihata pada materi dalam bentuk arsip. Berbagai arsip itu seperti teks (berupa bacaan), rekaman audio, atau dalam bentuk audio visual. Segala ini biasa ditemui saat melaksanakan penelitian tentang naskah, karya sastra, dan seni pertunjukan [5].

2.4. Metode Penetration Testing

Penetration Testing (*Pentest*) merupakan aktivitas dimana seseorang membuktikan dengan mensimulasikan serangan terhadap sistem jaringan. Orang yang melaksanakan kegiatan ini dikenal sebagai penguji penetrasi [8]. *Penetration Testing* dapat diartikan sebagai sebuah cara yang legal dan formal untuk mendapatkan dan mengeksploitasi sistem komputer yang bertujuan untuk menciptakan sistem yang jauh lebih aman [10]. Tetapi pada beberapa persoalan, kerentanan

yang didapat dari penguji penetrasi malah dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu sangat vital untuk memohonkan izin kepada pihak yang ingin di penguji penetrasi.



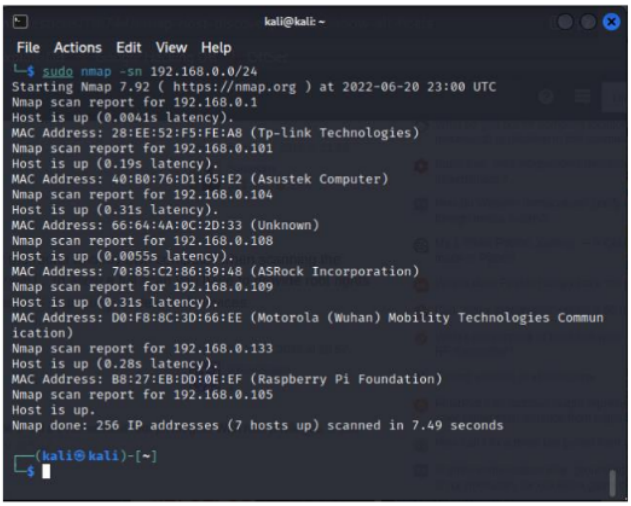
Gambar 1. Metode Penetration Testing

Gambar 1 menjelaskan, tingkatan dari metode *penetration testing* yang terdiri dari lima tahapan yakni mula-mula pada tahapan *Reconnaissance,* yaitu tahapan menetapkan tujuan pengujian menentukan ruang lingkup pengujian. Kemudian pada tingkatan *Scanning* atau memindai sasaran yaitu tahapan pencarian celah keamanan yang bisa digunakan untuk masuk ke dalam sistem menggunakan *tools-tools* yang ada. Kemudian pada tingkatan *Gaining Access* yaitu pengujian menerobos masuk ke dalam sistem dengan menggunakan teknik-teknik tertentu, pada penelitian ini digunakan *sniffing* dengan tujuan mengeksploitasi celah keamanan sistem, mencuri data yang ada pada sistem, memantau lintas *traffic* jaringan yang berlangsung, dan monitoring kegiatan yang ada pada objek yang diteliti. Kemudian pada tingkatan *Maintaining access*, yaitu apakah akses yang sudah didapatkan pada prosedur sebelumnya dapat ditutup sehingga keamanan pada sistem tetap aman. Dan tahap terakhir *Reporting* seperti pembuatan laporan dari rangkaian kegiatan yang sudah dilakukan

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

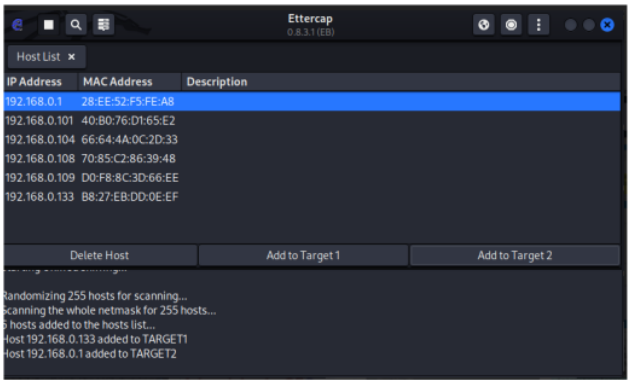
Berdasarkan analisis dan perancangan langkah pertama dalam *Penetration Testing* adalah *reconnaissance* yaitu mengumpulkan informasi yang diperlukan seperti mengumpulkan informasi perangkat *IoT* yang digunakan dan men scan *port* yang digunakan. Digunakan *tools* nmap pada kali linux yang terhubung dengan jaringan yang sama pada *target* seperti pada Gambar 2.



Gambar 2. Scanning IP and MAC address in the same network with nmap

Berdasarkan Gambar 2, dengan menggunakan *nmap* proses pengumpulan informasi didapat bahwa *IP address* perangkat *IoT* yang terhubung pada jaringan yang sama memiliki *IP* 192.168.0.105 dengan *MAC Address* B8:27:EB:DD:0E:FF dan informasi router yang terhubung memiliki *IP address 192.168.0.1* dengan *MAC Address* 28:EE:52:F5:FE:A8. Informasi ini diperlukan untuk melakukan serangan *MITM* menggunakan Ettercap Filter.

Pada Ettercap lakukan *scanning* pada jaringan maka akan muncul *ARP table* seperti pada Gambar 3.



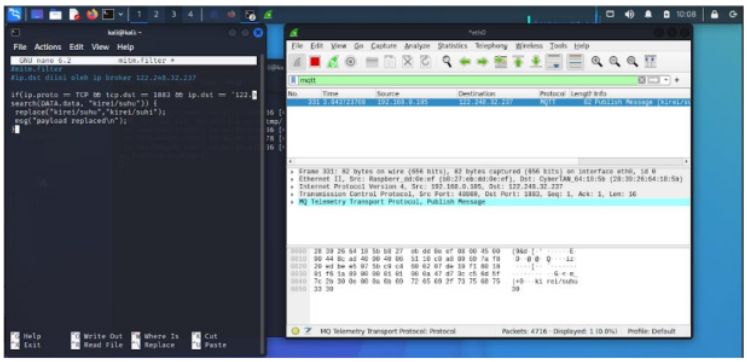
Gambar 3. list ARP table pada Ettercap

Berdasarkan Gambar 3, *IP* 192.168.0.133 dan *IP* 192.168.0.1 dipilih dan dimasukkan sebagai target 1 dan target 2. Setelah dijadikan target maka pilih Serangan *ARP Poisoning* maka serangan sedang berjalan. *ARP Poisoning* berjalan atau tidak dapat dideteksi pada raspberry dengan cara memasukkan perintah "arp –a" pada terminal maka pada IP yang berbeda memiliki *MAC Address* yang sama seperti pada Gambar 4,

```
pi@raspberrypi:~ $ arp -a
? (192.168.0.105) at 28:39:26:64:18:5b [ether] on wlan0
? (192.168.0.124) at 28:39:26:64:18:5b [ether] on wlan0
? (192.168.0.1) at 28:39:26:64:18:5b [ether] on wlan0
pi@raspberrypi:~ $
```

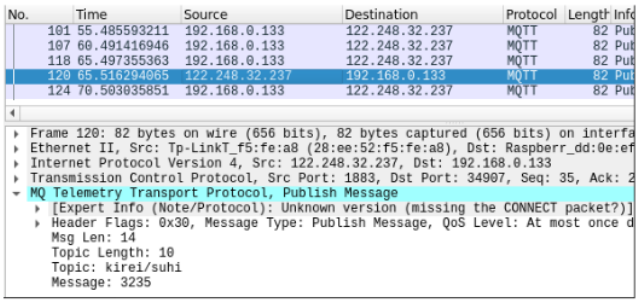
Gambar 4. ARP Poisoning berjalan

Setelah melakukan *ARP Poisoning* maka penyerang dapat melakukan *MITM,* untuk mengimplementasikan *MITM* digunakan Ettercap filter dan baris kode seperti pada Gambar 5.



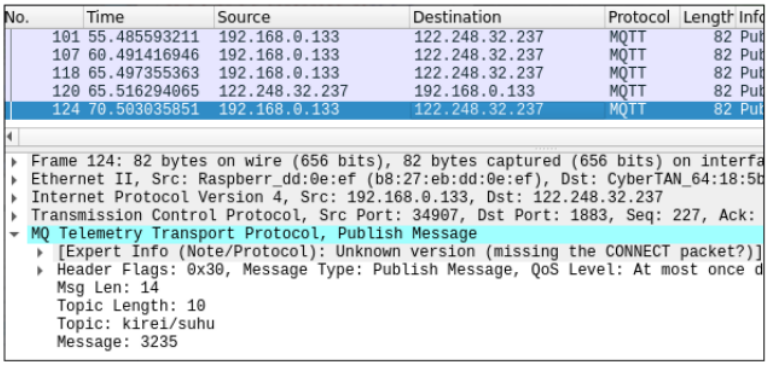
Gambar 5. memasukkan variabel hasil ARP Poisoning ke Ettercap Filter

Variabel 'IP broker' menggunakan hasil dari *ARP Poisoning* yang dapat mengetahui *IP broker* yang digunakan Smart Greenhouse, untuk mengganti data ketika proses transmisi data perlu diketahui data apa yang sedang dikirim, dengan menggunakan bantuan *tools* Wireshark dapat mendeteksi data yang dikirim melalui protokol *MQTT* berupa *plain text*. "kirei/suhu" adalah data yang dikirim ke server. Variabel tersebut dimasukkan kedalam baris kode gambar x dan variabel yang menjadi pengganti data adalah "kirei/suhi". Setelah semua variabel dimasukkan. Maka kode program akan di-*compile* dan dijalankan oleh Ettercap Filter. Untuk mengetahui apakah serangan berhasil dilakukan maka akan diperiksa kembali transmisi data *MQTT* menggunakan Wireshark yang ditunjukkan pada Gambar 6 dan 7. Pada Gambar 6 transmisi data dari *server broker* ke perangkat *Raspberry* mengalami perbedaan data dengan yang ditunjukkan Pada Gambar 7



Gambar 6. MITM berhasil mengubah data integrity

Pada Gambar 6 transmisi data dari *server broker* ke perangkat *Raspberry* mengalami perbedaan data dengan yang ditunjukkan Pada Gambar 7.



Gambar 7. MITM berhasil mengubah data integrity

Berdasarkan analisis dan implementasi yang telah dilakukan didapat beberapa celah *MQTT* yang didapat yang ditunjukkan pada Tabel IV. 5

Tabel IV. 1 Celah Keamanan MQTT

No	Nama Serangan	Status
1	*Search Engine* Shodan	Gagal
2	*ARP Poisoning*	Berhasil
3	*MITM Attack*	Berhasil

Sedangkan pada *MQTTS* yang didapat yang ditunjukkan pada Tabel IV. 6

Tabel IV. 2 Celah Keamanan MQTTS

No	Nama Serangan	Status
1	*Search Engine* Shodan	Gagal
2	*ARP Poisoning*	Gagal
3	*MITM Attack*	Gagal

Berdasarkan studi literatur, hal ini terjadi karena pada protokol *MQTTS, MQTT* "dibungkus" oleh *TLS,* sehingga ketika pada proses transmisi data meskipun penyerang melakukan *sniffing*, penyerang tidak dapat menemukan informasi apapun dikarenakan data baru dapat dibaca ketika data telah sampai pada tujuan. Untuk kasus ini data telah sampai pada server *MQTT* dan server akan melakukan serangkaian tindakan untuk membukanya seperti memeriksa *certificate authentication, handshake, alert, changecipherspec,* dan *encryption*.

4. KESIMPULAN

Berdasarkan hasil analisis dan implementasi, protokol *MQTT* memiliki celah keamanan berupa serangan *ARP Poisoning* dan *MITM Attack*. Serangan tersebut tidak dapat dilakukan pada protokol *MQTTS*.

.

DAFTAR PUSTAKA

[1] Simon Kemp, 5 April 2022, Digital 2022 Indonesia :Internet use in Indonesia 2022, https://datareportal.com/reports/digital-2022 indonesia?rq=indonesia%202022.

[2] N. Rohman, R. Luviana Musyarofah, E. Utami, and S. Raharjo, "Natural Language Processing on Marketplace Product Review Sentiment Analysis," in 2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS), 2020, pp. 1–5, doi: 10.1109/ICORIS50180.2020.9320827.

[3] X. Wang, T. Zhou, X. Wang, and Y. Fang, "Harshness-aware sentiment mining framework for product review," Expert Systems with Applications, vol. 187, p. 115887, 2022, doi: https://doi.org/10.1016/j.eswa.2021.115887.

[4] J.-W. Bi, Y. Liu, and Z.-P. Fan, "Representing sentiment analysis results of online reviews using interval type-2 fuzzy numbers and its application to product ranking," Information Sciences, vol. 504, pp. 293–307, 2019, doi: https://doi.org/10.1016/j.ins.2019.07.025.

[5] Q. Wang, W. Zhang, J. Li, F. Mai, and Z. Ma, "Effect of online review sentiment on product sales: The moderating role of review credibility perception," Computers in Human Behavior, vol. 133, p. 107272, 2022, doi: https://doi.org/10.1016/j.chb.2022.107272.

[6] Kevin, V. et al. (2020) "Analisis Sentimen Transportasi Online Menggunakan Support Vector Machine Berbasis Particle Swarm Optimization (Online Transportation Sentiment Analysis Using Support Vector Machine Based on Particle Swarm Optimization)," Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 9(2), hal. 162–170FLEXChip Signal Processor (MC68175/D), Motorola, 1996.

[7] Y. Yennimar and R. Rizal, “Comparison of Machine Learning Classification Algorithms in Sentiment Analysis Product Review of North Padang Lawas Regency,” SinkrOn, vol. 4, p. 268, 2019, doi: 10.33395/sinkron.v4i1.10416

[8] Sihombing, L., Hannie, H. dan Dermawan, B. (2021) “Sentimen Analisis Customer Review Produk Shopee Indonesia Menggunakan Algortima Naïve Bayes Classifier,” Edumatic: Jurnal Pendidikan Informatika, 5, hal. 233–242. doi: 10.29408/edumatic.v5i2.4089

[9] M. T. Akter, M. Begum, and R. Mustafa, “Bengali Sentiment Analysis of E-commerce Product Reviews using K-Nearest Neighbors,” in 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), 2021, pp. 40–44, doi: 10.1109/ICICT4SD50815.2021.9396910

[10] S. F. N. H. R. JAYADI, “Sentiment Analysis Of Indonesian E-Commerce Product Reviews Using Support Vector Machine Based Term Frequency Inverse Document,” vol. 99, no. 17, pp. 4316–4325, 2022

cory v3

ORIGINALITY REPORT

9%	7%	3%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.scribd.com Internet Source	2%
2	Erwin Raza, La Ode Sabaruddin, Aziza Leila Komala. "Manfaat dan Dampak Digitalisasi Logistik di Era Industri 4.0", Jurnal Logistik Indonesia, 2020 Publication	2%
3	core.ac.uk Internet Source	1%
4	www.damang.web.id Internet Source	1%
5	aliyhafiz.com Internet Source	1%
6	ejournal.poltektegal.ac.id Internet Source	1%
7	yahya4ever.blogspot.com Internet Source	1%
8	Devi Efriadi, Rahmaddeni Rahmaddeni, Agustin Agustin, Junadhi Junadhi. "Prediksi	1%

	Penambahan Piutang Iuran Jaminan Sosial Ketenagakerjaan menggunakan Algoritma K-Nearest Neighbor", Edumatic: Jurnal Pendidikan Informatika, 2022 Publication	
9	ftid.lpkia.ac.id Internet Source	1 %
10	repositori.uin-alauddin.ac.id Internet Source	1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

SERTIFIKAT

Direktorat Jenderal Pendidikan Tinggi, Riset dan Teknologi
Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi Republik Indonesia

Kutipan dari Keputusan Direktorat Jenderal Pendidikan Tinggi, Riset dan Teknologi
Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia

Nomor 105/E/KPT/2022
Peringkat Akreditasi Jurnal Ilmiah Periode 1 Tahun 2022

Nama Jurnal Ilmiah

Smart Comp :Jurnalnya Orang Pintar Komputer

E-ISSN: 25490796

Penerbit: PUSAT PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT (P3M) POLITEKNIK HARAPAN BERSAMA

Ditetapkan Sebagai Jurnal Ilmiah

TERAKREDITASI PERINGKAT 4

Akreditasi Berlaku selama 5 (lima) Tahun, yaitu
Volume 10 Nomor 1 Tahun 2021 Sampai Volume 14 Nomor 2 Tahun 2025

Jakarta, 07 April 2022
Plt. Direktur Jenderal Pendidikan Tinggi,
Riset, dan Teknologi

Prof. Ir. Nizam, M.Sc., DIC, Ph.D., IPU, ASEAN Eng
NIP. 196107061987101001

DOI: https://doi.org/10.30591/smartcomp.v12i4.4681