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

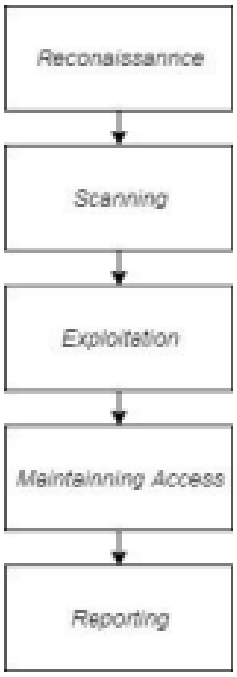
Perangkat wawancara digunakan dalam penelitian kualitatif karena dapat menyingkap informasi lintas waktu seperti waktu lampau, waktu sekarang, maupun waktu depan. Data yang dimanifestasikan dari wawancara bersifat terbuka, menyeluruh, dan tidak terbatas, sehingga sanggup membentuk informasi yang utuh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



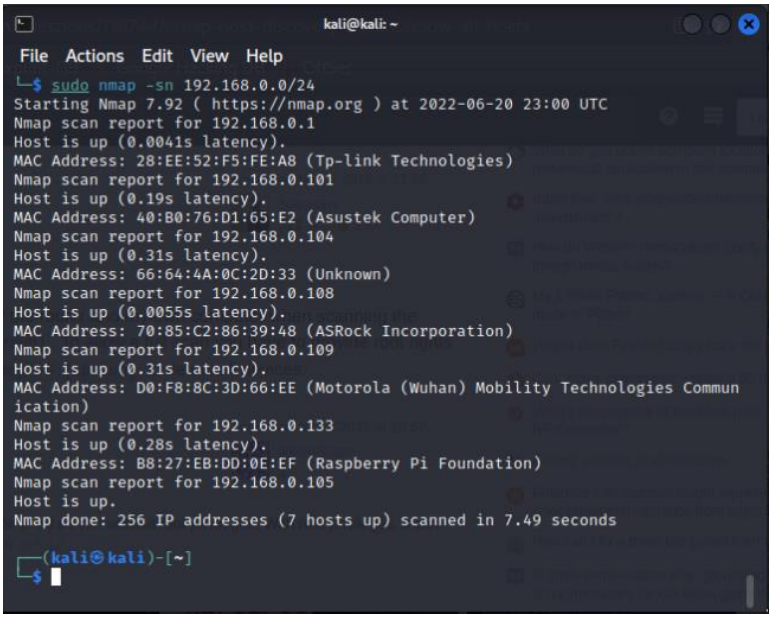
Gambar 1. Metode Penetration Testing

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

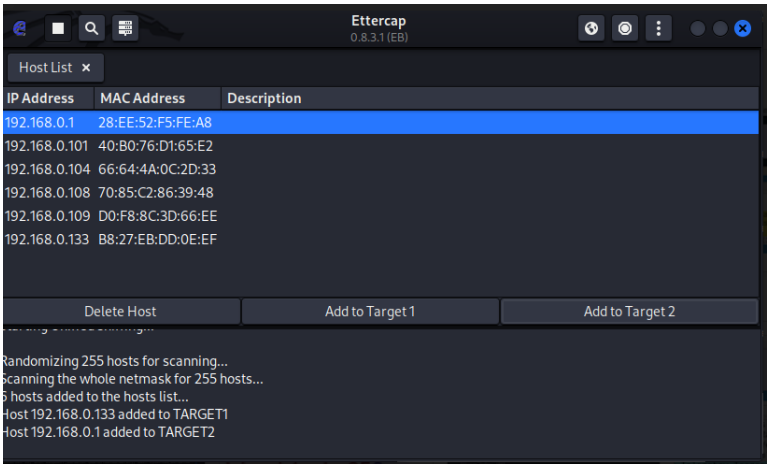
Berdasarkan analisis dan perancangan langkah pertama dalam *Penetration Testing* adalah *reconnaissance* yaitu mengumpulkan informasi yang diperlukan seperti mengumpulkan informasi perangkat *IoT* yang digunakan dan men scan *port* yang digunakan. Digunakan *tools* nmap pada kali linux yang terhubung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



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

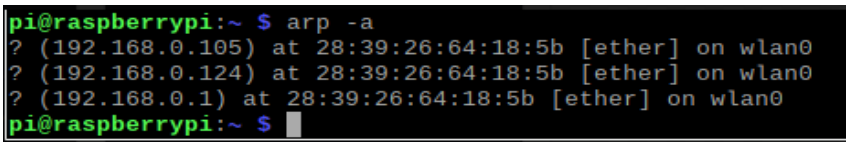
Berdasarkan Gambar 2, dengan menggunakan *nmap* proses pengumpulan informasi didapat bahwa *IP address* perangkat *IoT* yang terhubung pada jaringan yang sama memiliki *IP* 192.168.0.105 dengan *MAC Address* B8:27:EB:DD:0E:FF dan informasi router yang terhubung memiliki *IP address 192.168.0.1* dengan *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.



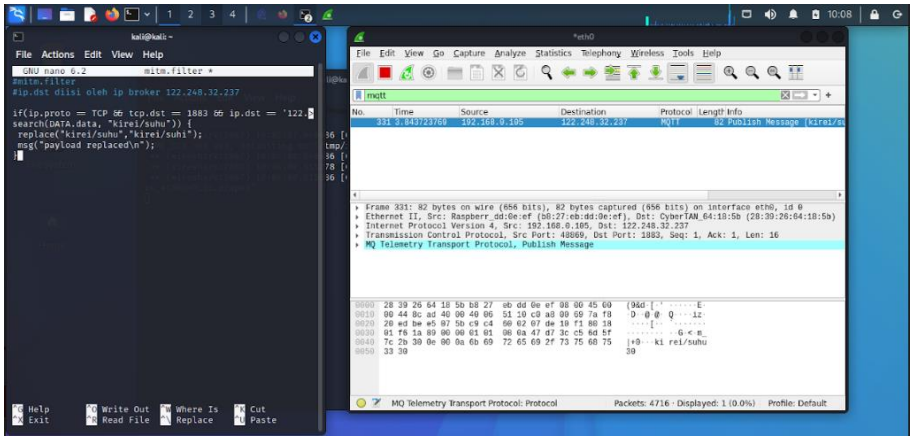
Gambar 3. list ARP table pada Ettercap

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,



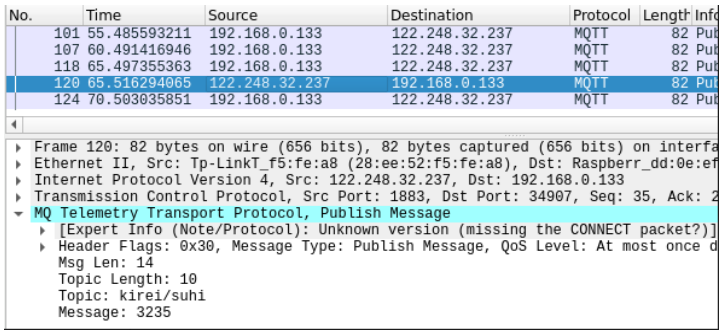
Gambar 4. ARP Poisoning berjalan

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



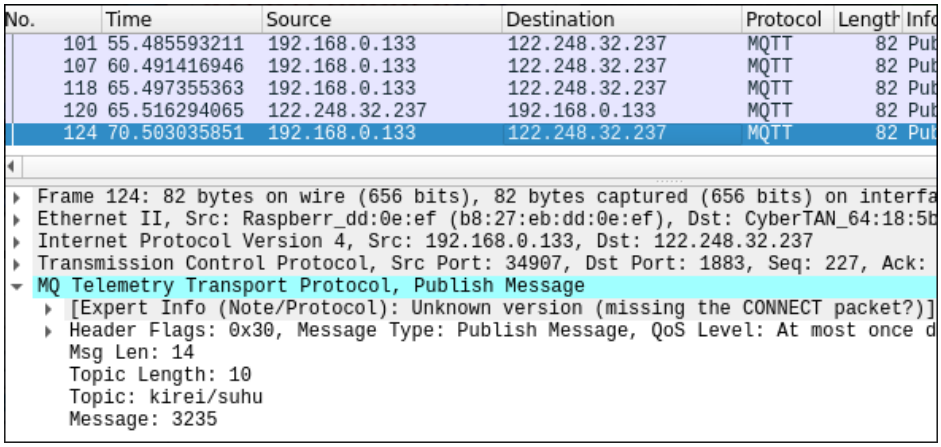
Gambar 5. memasukkan variabel hasil ARP Poisoning ke Ettercap Filter

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