Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari

OPEN ACCESS

https://doi.org/10.63447/jimik.v7i1.1625

Analisis Kelemahan Fitur *Cloud* pada *Access Point* Berbasis *Cloud*

Kaiva Alby Aufinanta [1*]

[1*] Program Studi Teknik Informatika, Univeristas Kristen Satya Wacana, Kota Salatiga, Provinsi Jawa Tengah, Indonesia.

Corresponding Email: kaivaalbyu38@gmail.com [1*]

Histori Artikel:
Dikirim 22 Agustus 2025; *Diterima dalam bentuk revisi* 12 September 2025; *Diterima* 10 Oktober 2025; *Diterbitkan* 10 Januari 2026.

Abstrak

Penelitian bertujuan mengidentifikasi dan menganalisis kerentanan fitur Cloud pada Access Point melalui pendekatan eksperimental. Fitur Cloud pada Access Point mencakup pengelolaan sumber daya jaringan, penyimpanan, pemrosesan data, serta layanan manajemen perangkat berbasis internet yang digunakan untuk memantau lalu lintas perangkat, memperbarui firmware, dan melakukan konfigurasi terpusat. Tahapan penelitian diawali dengan perancangan konfigurasi Access Point, diikuti simulasi serangan Man-in-the-Middle (MITM) menggunakan metode SSL Strip. Pengujian dilakukan menggunakan Access Point Ruijie Reyee RG-EW1200 dengan dukungan perangkat lunak Bettercap pada sistem operasi Kali Linux dan mesin virtual Windows. Proses penelitian meliputi identifikasi fitur Cloud pada perangkat, pengumpulan dokumentasi teknis, pelaksanaan simulasi serangan SSL Strip, dan analisis kerentanan yang ditemukan. Hasil eksperimen menunjukkan kerentanan spesifik pada sistem keamanan Cloud Access Point berupa kebocoran data Password, SSID, IP, Serial Number, Network Name, Tipe Device, Versi Firmware, MAC Address, Forward Mode, Status Access Point, dan Status Port yang kemudian dianalisis untuk memberikan rekomendasi mitigasi. Temuan diharapkan dapat menjadi referensi dalam peningkatan keamanan fitur Cloud pada perangkat jaringan, khususnya Access Point berbasis manajemen terpusat.

Kata Kunci: Keamanan Cloud; SSL Strip; Man-in-the-Middle; Access Point; Kerentanan Jaringan.

Abstract

This study aims to identify and analyze vulnerabilities of Cloud features in Access Points through an experimental approach. Cloud features in Access Points include network resource management, storage, data processing, and internet-based device management services used to monitor device traffic, update firmware, and perform centralized configuration. The research began with the design of Access Point configurations, followed by a simulation of a Man-in-the-Middle (MITM) attack using the SSL Strip method. Testing was conducted using a Ruijie Reyee RG-EW1200 Access Point with the support of Bettercap software on the Kali Linux operating system and a Windows virtual machine. The research process involved identifying Cloud features of the device, collecting technical documentation, executing SSL Strip attack simulations, and analyzing discovered vulnerabilities. Experimental results revealed specific vulnerabilities in the Cloud security system of the Access Point, including data leakage of Password, SSID, IP, Serial Number, Network Name, Device Type, Firmware Version, MAC Address, Forward Mode, Access Point Status, and Port Status, which were then analyzed to provide mitigation recommendations. These findings are expected to serve as a reference for enhancing security of Cloud features in network devices, particularly centralized management-based Access Points.

Keyword: Cloud Security; SSL Strip; Man-in-the-Middle; Access Point; Network Vulnerability.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

1. Pendahuluan

Dunia teknologi, khususnya jaringan berbasis *Cloud*, telah berkembang pesat dalam beberapa tahun terakhir untuk mendukung berbagai aktivitas, mulai dari pengelolaan data hingga infrastruktur jaringan. Transformasi digital ini mendorong adopsi teknologi *Cloud Computing* yang menawarkan fleksibilitas, skalabilitas, dan efisiensi dalam pengelolaan sumber daya teknologi informasi. Salah satu implementasi teknologi *Cloud* yang semakin populer adalah fitur *Cloud Management* pada perangkat jaringan, khususnya *Access Point*, yang memungkinkan administrator jaringan untuk mengelola perangkat dari jarak jauh dengan lebih mudah dan efisien. Fitur *Cloud* pada *Access Point* dirancang untuk memudahkan pengguna dalam melakukan *monitoring* maupun konfigurasi perangkat secara terpusat tanpa harus berada di lokasi fisik perangkat. Platform manajemen berbasis *Cloud* ini memiliki berbagai kemampuan canggih, seperti *multi-site management* yang memungkinkan pengelolaan beberapa lokasi sekaligus, *monitoring* secara *real-time* untuk memantau kondisi jaringan secara langsung, serta analisis performa atau kelayakan pada *device* yang membantu dalam pengambilan keputusan strategis terkait infrastruktur jaringan (Dedi Gunawan, September 2023). Kemudahan akses dan kontrol terpusat ini menjadikan fitur *Cloud* sebagai solusi yang menarik bagi organisasi yang memiliki infrastruktur jaringan tersebar di berbagai lokasi geografis.

Namun, di balik kemudahan dan efisiensi yang ditawarkan, fitur *Cloud* pada *Access Point* tidak terlepas dari berbagai risiko keamanan yang perlu mendapat perhatian serius. Kerentanan terhadap data pengguna dan serangan siber menjadi ancaman nyata yang dapat mengeksploitasi kelemahan sistem. Selain itu, konfigurasi pada *Access Point* yang kurang optimal atau tidak mengikuti *best practice* keamanan menjadi salah satu celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan terhadap sistem. *Access Point* sendiri merupakan perangkat keras (*hardware*) yang digunakan dalam jaringan lokal nirkabel untuk menyampaikan dan menerima data, menghubungkan antar pengguna dalam satu jaringan, serta berfungsi sebagai jembatan koneksi antara *Wireless Local Area Network* (WLAN) dan jaringan kabel (Ahmad Martani, Oktober 2023). Beberapa penelitian terdahulu telah mengidentifikasi berbagai kelemahan pada sistem *Cloud Management* untuk perangkat jaringan. Ancaman yang teridentifikasi berupa serangan *Distributed Denial of Service* (DDoS) yang dapat melumpuhkan layanan, serangan *Man-in-the-Middle* (MITM) yang dapat menyadap komunikasi data, kebocoran data pengguna yang mengancam privasi dan keamanan informasi, serta konfigurasi yang kurang aman yang membuka celah bagi penyerang (Aryanto Nur, 2024). Risiko-risiko ini dapat menyebabkan perangkat terhubung ke jaringan publik secara tidak aman karena menggunakan mekanisme autentikasi yang lemah atau protokol komunikasi yang tidak terenkripsi dengan baik. Kelemahan fundamental ini dapat berdampak signifikan pada performa dan keamanan jaringan, terutama saat jaringan mengalami gangguan atau masalah teknis, di mana kondisi tersebut justru dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melancarkan serangan.

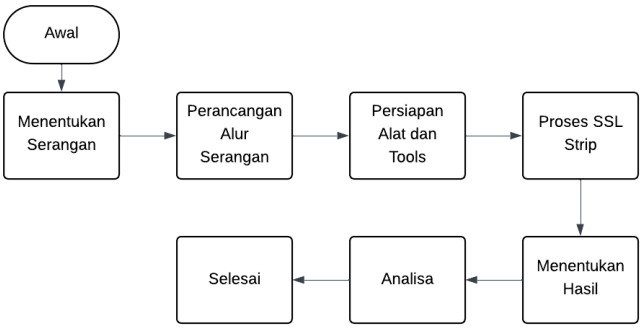
Penelitian ini bertujuan untuk melakukan pengujian keamanan terhadap fitur *Cloud* pada *Access Point* melalui simulasi serangan *SSL Strip*, sebuah teknik serangan yang memanfaatkan kelemahan dalam implementasi protokol keamanan *Secure Sockets Layer/Transport Layer Security* (SSL/TLS). Fokus utama penelitian adalah menguji keamanan sistem dan mengidentifikasi apakah data sensitif berupa *password* login dan informasi konfigurasi dari *Access Point* Ruijie dapat diintersepsi atau disadap melalui metode serangan *Man-in-the-Middle*. Pemilihan *Access Point* Ruijie Reyee RG-EW1200 sebagai objek penelitian didasarkan pada popularitas penggunaan perangkat ini di berbagai organisasi dan institusi, serta fitur *Cloud Management* yang terintegrasi dalam sistem perangkat. Dengan memahami secara mendalam kelemahan dan kerentanan yang ada pada sistem *Cloud Management* untuk *Access Point*, diharapkan penelitian ini dapat memberikan kontribusi berupa solusi mitigasi yang efektif dan rekomendasi *best practice* dalam penggunaan fitur *Cloud* pada perangkat jaringan. Temuan penelitian ini juga diharapkan dapat menjadi bahan pertimbangan bagi vendor perangkat jaringan untuk meningkatkan aspek keamanan produk mereka, serta memberikan kesadaran kepada administrator jaringan tentang pentingnya implementasi konfigurasi keamanan yang tepat dalam lingkungan jaringan berbasis *Cloud*.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

2. Metode Penelitian

Penelitian ini menggunakan metode eksperimental untuk mengidentifikasi dan menganalisis kelemahan fitur *Cloud* pada *Access Point*. *Cloud* pada *Access Point* ini adalah model seperti sumber daya jaringan, penyimpanan, pengolahan data, dan layanan manajemen *device* yang disediakan melalui internet. Di dalam *Access Point*, teknologi ini digunakan untuk memantau *traffic* perangkat, *update firmware*, dan konfigurasi terpusat (Muhamad Agil Faizi, Agustus 2024). Penelitian dilakukan dengan pengujian langsung terhadap *device* dan platform *Cloud* yang relevan. Langkah pertama yang akan dilakukan dalam penelitian ini berupa merancang konfigurasi *Access Point*, lalu memberikan simulasi serangan berupa *Man-in-the-Middle* (MITM). Kemudian metode yang digunakan adalah *SSL Strip*. *SSL Strip* adalah serangan yang dibuat oleh Moxie Marlinspike pada tahun 2009 dan telah dipresentasikan di acara konferensi *BlackHat DC 2009*. *SSL Stripping* adalah teknik menghilangkan data *SSL/TLS* dari sebuah *request message* (Nathanael Dharmawan, 2022). Selanjutnya adalah penggunaan *device Access Point* Ruijie Reyee RG-EW1200. Pemilihan perangkat ini dikarenakan harga yang terjangkau, ketersediaan barang yang mudah, dan perangkat mudah didapatkan di pasaran. Tahap berikutnya adalah menginstal *tools* berupa *Bettercap* di *Operating System* Kali Linux dan membuat *Virtual Machine* Windows. *Bettercap* adalah *software* yang masuk dalam kategori *open source* dan *tools* keamanan jaringan untuk serangan *Man-in-the-Middle*. Aplikasi tersebut hanya berjalan pada jaringan LAN dengan cara kerja menganalisis suatu jaringan protokol komputer dan mengumpulkan informasi paket yang dikirim dan diterima oleh komputer lain (Yacob Hae, 2021).

Langkah penelitian ini diawali dengan pengumpulan data berupa identifikasi fitur *Cloud* pada *device* dan dokumentasi teknis terkait keamanan fitur *Cloud*. Selanjutnya adalah tahap simulasi yang meliputi simulasi serangan *SSL Strip* untuk menguji kerentanan *Cloud*. Tahap terakhir adalah menentukan hasil dan analisis data eksperimen yang diidentifikasi kelemahannya secara spesifik. Hasil eksperimen ini akan dianalisis untuk mengidentifikasi kelemahan utama dan memberikan solusi mitigasi yang tepat guna meningkatkan keamanan sistem *Cloud Management* pada *Access Point*.



Gambar 1. Model Proses Penelitian.

3. Hasil dan Pembahasan

3.1 Hasil

Pada penelitian ini telah dilakukan pengujian keamanan terhadap fitur *Cloud* pada *Access Point* Ruijie Reyee RG-EW1200 menggunakan metode *SSL Strip* untuk mengidentifikasi potensi ancaman keamanan yang dapat mengeksploitasi kelemahan sistem. Hasil pengujian menunjukkan bahwa serangan *SSL Strip* berhasil dilaksanakan dan berdampak signifikan terhadap keamanan data pengguna *Access Point* tersebut. Dari *log status* yang tercatat pada *tools Bettercap*, ditemukan berbagai data sensitif yang berhasil disadap, meliputi *Password*, SSID, IP, *Serial Number*, *Network Name*, Tipe *Device*, Versi *Firmware*, *MAC Address*, *Forward Mode*, Status *Access Point*, dan Status Port *Access Point* Ruijie.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

Keberhasilan intersepsi data-data sensitif ini menunjukkan bahwa penyerang berpotensi melakukan pencurian data (*data theft*), mengakses konfigurasi perangkat secara tidak sah, dan melancarkan serangan lebih lanjut yang dapat membahayakan integritas dan keamanan jaringan secara keseluruhan. Data yang berhasil disadap ini merupakan informasi kritis yang seharusnya dilindungi dengan enkripsi yang kuat, namun kelemahan dalam implementasi protokol keamanan menyebabkan data tersebut dapat diintersepsi dalam bentuk *plaintext*. Dalam simulasi serangan *SSL Strip* pada jaringan, teknik yang digunakan adalah menurunkan tingkat keamanan koneksi URL dari HTTPS menjadi HTTP agar penyerang dapat mengintersepsi dan membaca data yang dikirimkan oleh pengguna *Access Point* tanpa terdeteksi. Mekanisme serangan ini memanfaatkan kelemahan dalam proses *handshake* SSL/TLS dan kemampuan untuk memanipulasi *traffic* jaringan melalui serangan *Man-in-the-Middle* (MITM). Dengan menggunakan *tools Bettercap* yang dikonfigurasi secara khusus, penelitian ini berhasil membuktikan bahwa *Access Point* Ruijie masih memiliki kelemahan keamanan yang signifikan. Setelah dilakukan serangkaian pengujian dan analisis mendalam, ditemukan bahwa *Access Point* Ruijie ini rentan terhadap serangan *SSL Strip* karena tidak menerapkan mekanisme perlindungan yang memadai seperti *HTTP Strict Transport Security* (HSTS) atau validasi sertifikat yang ketat. Temuan ini mengonfirmasi bahwa meskipun fitur *Cloud Management* menawarkan kemudahan dalam pengelolaan perangkat, aspek keamanan masih memerlukan perbaikan dan penguatan untuk melindungi data pengguna dari ancaman serangan siber yang semakin canggih.

3.2 Pembahasan

Pada metode *SSL Strip* ini memiliki beberapa langkah yang cukup kompleks, meliputi persiapan *tools*, *Operating System* berupa *virtual machine* yang diinstal melalui Oracle VirtualBox, dan konfigurasi *Access Point* Ruijie Reyee RG-EW1200 sebagai target pengujian. Kompleksitas tahapan ini memerlukan pemahaman mendalam tentang arsitektur jaringan, protokol keamanan, dan teknik serangan siber untuk memastikan simulasi berjalan sesuai dengan skenario yang direncanakan. Berikut adalah langkah-langkah detail dalam pembuatan dan pelaksanaan serangan *SSL Strip*:

3.2.1 Instal *Operating System* Kali Linux dan Windows

Langkah ini adalah tahap awal dari pembuatan simulasi *SSL Strip* karena pelaksanaan serangan menggunakan OS (*Operating System*) Kali Linux sebagai platform penyerang, sedangkan fungsi dari Windows adalah sebagai *target* atau *victim* untuk memvalidasi bahwa serangan ini berjalan dengan sukses atau tidak. OS (*Operating System*) merupakan program yang mengendalikan jalannya program-program aplikasi dan berfungsi sebagai jembatan penghubung antara pengguna dengan perangkat keras komputer (Satriawaty Mallu, 2024). Kali Linux dipilih karena sistem operasi ini dirancang khusus untuk keperluan *penetration testing* dan *security auditing*, dilengkapi dengan berbagai *tools* keamanan yang telah terinstal secara *default*, sehingga memudahkan peneliti dalam melakukan simulasi serangan. Sementara itu, Windows digunakan sebagai sistem operasi *victim* karena merepresentasikan lingkungan pengguna umum yang sering menjadi target serangan dalam dunia nyata.

3.2.2 Memulai Instalasi Penyerangan pada OS Kali Linux

Buka Kali Linux lalu klik tombol *search* dan ketik *terminal* karena instalasi dan eksekusi penyerangan menggunakan media *terminal* atau *command line interface*. Setelah dibuka dan masuk ke *terminal*, lalu ketik sudo apt-get install bettercap untuk melakukan instalasi *tools Bettercap*. Proses instalasi ini akan mengunduh dan mengonfigurasi semua dependensi yang diperlukan untuk menjalankan *Bettercap* dengan optimal. Setelah berhasil menginstal *tools Bettercap*, masukkan perintah untuk IP *forwarding* dengan mengetik echo 1 > /proc/sys/net/ipv4/ip_forward. Perintah ini bertujuan untuk mengaktifkan *packet forwarding* di OS agar *tools Bettercap* dapat mengalihkan dan memanipulasi *traffic* jaringan menjadi serangan *Man-in-the-Middle* tanpa memutuskan koneksi jaringan pada target, sehingga korban tidak menyadari bahwa komunikasi mereka sedang disadap. Aktivasi IP *forwarding* ini sangat krusial karena tanpa fitur ini, paket data tidak akan diteruskan antara korban dan *gateway*, yang akan menyebabkan koneksi terputus dan membuat serangan mudah terdeteksi.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

3.2.3 Menjalankan *Interface* Jaringan di *Bettercap*

Untuk langkah selanjutnya adalah menjalankan *interface* jaringan dengan memasukkan perintah di *terminal*, ketik sudo bettercap -iface eth0 karena *interface* yang digunakan adalah *ethernet*, maka pada perintah tersebut dimasukkan eth0. Jika *interface* jaringan menggunakan *Wireless*, dapat diganti dengan wlan0 sesuai dengan konfigurasi jaringan yang digunakan. Jika belum mengetahui *interface* jaringan yang aktif pada OS, dapat memasukkan perintah ip a atau ifconfig untuk mengecek dan mengidentifikasi *interface* yang tersedia beserta konfigurasi IP-nya. Pemilihan *interface* yang tepat sangat penting untuk memastikan bahwa *Bettercap* dapat menangkap dan memanipulasi *traffic* pada jaringan yang benar, karena kesalahan dalam memilih *interface* akan menyebabkan serangan tidak berfungsi sebagaimana mestinya.

3.2.4 Mengaktifkan Perintah untuk Serangan di *Bettercap*

Jika sudah masuk di *interface* jaringan di *tools Bettercap*, masukkan perintah net.probe on. Perintah ini adalah modul dari *discovery* aktif untuk mencari dan mengidentifikasi *host* pada jaringan yang sedang digunakan, sehingga penyerang dapat mengetahui perangkat mana saja yang terhubung dalam jaringan tersebut. Proses selanjutnya adalah menentukan target sasaran berupa IP target yang telah ditentukan. Pada penelitian ini, target IP yang digunakan adalah 10.40.4.11 yang merupakan IP dari *Access Point* Ruijie. Langkah ini dilakukan dengan memasukkan perintah set arp.spoof.targets 10.40.4.11 lalu tekan *enter*, kemudian mengaktifkan *arpspoof* tersebut dengan memasukkan perintah arp.spoof on lalu *enter* dan *arpspoof* akan aktif. *Arpspoof* ini bertujuan untuk memanipulasi tabel ARP (*Address Resolution Protocol*) dengan mengisolasi alamat MAC penyerang dan mengaitkannya dengan alamat IP dari *host* lain seperti *gateway default*, sehingga menyebabkan lalu lintas yang dimaksudkan untuk alamat IP tersebut dikirim ke penyerang sebagai gantinya atau melakukan tindakan yang tidak diinginkan (Rifan Ramadhan Chandra Dirgantara, 2020). Setelah memilih IP target, selanjutnya adalah mengaktifkan fitur *SSL Strip* di modul *proxy* dengan memasukkan perintah set http.proxy.sslstrip true yang berfungsi untuk menurunkan koneksi dari HTTPS ke HTTP agar dapat melihat isi data yang disadap dalam bentuk *plaintext*. Langkah selanjutnya adalah memasukkan perintah set http.proxy.sslstrip.obfuscate true yang berfungsi agar serangan tidak terdeteksi oleh korban dengan menyamarkan manipulasi yang dilakukan pada *traffic* jaringan. Lalu masukkan perintah set http.proxy.sslstrip.favicon true yang bertujuan untuk mengubah ikon pada *web browser* agar tampak seperti situs HTTPS yang aman, sehingga korban tidak curiga bahwa koneksi mereka telah diturunkan ke HTTP. Langkah terakhir untuk mengaktifkan *proxy* adalah dengan memasukkan perintah http.proxy on, yang akan mengaktifkan seluruh modul *proxy* dan memulai proses intersepsi *traffic*.

3.2.5 Melihat Isi Paket Data setelah Serangan Berhasil

Langkah untuk melihat data yang berhasil disadap dari serangan *SSL Strip* dapat dilakukan dengan mengaktifkan fitur *sniffing* pada *Bettercap*. Jika serangan pada umumnya dapat menampilkan data *username*, *password*, dan isi paket data secara langsung, namun pada penelitian ini fokus utama adalah menampilkan *Password*, SSID, IP, *Serial Number*, *Network Name*, Tipe *Device*, Versi *Firmware*, *MAC Address*, *Forward Mode*, Status *Access Point*, dan Status Port dari *Access Point* yang dikirimkan ke *Cloud*. Untuk mengetahui dan menampilkan data tersebut, dapat memasukkan perintah set net.sniff.verbose true lalu klik *enter*, dan perintah tersebut akan otomatis aktif untuk menampilkan detail paket yang tertangkap. Langkah untuk mengaktifkan *sniff* dapat dilakukan dengan memasukkan perintah net.sniff on, yang akan memulai proses penangkapan dan analisis paket data secara *real-time*. Pada serangan *SSL Strip* ini, dampak yang terjadi adalah akses *web* yang sebelumnya memiliki koneksi URL HTTPS berubah menjadi HTTP, sehingga data yang dikirimkan tidak lagi terenkripsi. Hal ini menjadi celah besar untuk masuknya serangan atau pencurian data karena semua informasi yang dikirimkan dapat dibaca dalam bentuk teks biasa (*plaintext*). Setelah dilakukan percobaan serangan pada penelitian ini, hasil yang ditampilkan pada Gambar 2 menunjukkan bahwa pada *log packet* yang telah didapat langsung dari *log terminal tools Bettercap*, data yang tertangkap berbentuk *plaintext* dan

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

menggunakan format data JSON, yang menunjukkan bahwa hasilnya berbentuk API (*Application Programming Interface*) yang digunakan untuk komunikasi antara *Access Point* dan server *Cloud*.

Gambar 2. Isi Paket Data di API

Gambar 3. Isi Paket Data

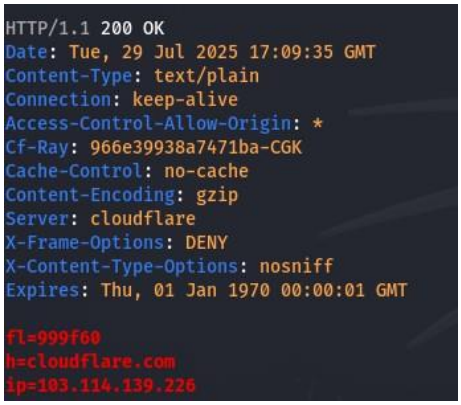
Pada Gambar 3, hasil ini menampilkan paket data yang dikirimkan ke *Cloud*, yaitu *password* dari *Access Point* Ruijie yang seharusnya dilindungi dengan enkripsi kuat namun berhasil disadap dalam bentuk *plaintext*. Lalu pada *log* selanjutnya menampilkan SSID, IP, *Serial Number*, *Network Name*, Tipe *Device*, Versi *Firmware*, *MAC Address*, *Forward Mode*, dan Status *Access Point* Ruijie. *Log* yang terakhir menampilkan status port dari *Access Point* Ruijie, yang memberikan informasi detail tentang port mana saja yang sedang aktif dan digunakan. Hasil ini juga akan ditampilkan di sistem *Cloud* Ruijie guna mengetahui port mana saja yang sedang digunakan dan mengetahui IP berapa yang sedang digunakan oleh port tersebut, sehingga administrator dapat melakukan *monitoring* dan manajemen perangkat secara terpusat. Namun, kelemahan keamanan yang teridentifikasi menunjukkan bahwa data-data sensitif ini dapat diintersepsi oleh pihak yang tidak berwenang, yang berpotensi menyebabkan kompromi keamanan jaringan secara menyeluruh.

3.2.5 Alur Data dalam Paket

Alur data yang ada dalam serangan *SSL Strip* ini dapat dijelaskan secara sistematis sebagai berikut. Pertama, ketika *Access Point* hendak dimasukkan ke *Cloud*, administrator harus membuat grup proyek dan memasukkan *Serial Number Access Point* untuk proses registrasi dan autentikasi perangkat. Selanjutnya, alur yang kedua adalah melihat *log* di *Bettercap*, dan yang terlihat pada *log terminal* adalah paket berupa *Work Mode*, SSID, *Serial Number*, dan data-data lain dari *Access Point*. Data ini akan secara otomatis dikirimkan dari *Cloud* yang meminta informasi ke *Access Point* karena di dalam *Cloud* nantinya akan ada proses sinkronisasi untuk memvalidasi bahwa data-data yang dikirim dari *Access Point* benar dan valid sesuai dengan konfigurasi yang terdaftar. Alur yang ketiga adalah ketika *Access Point* sudah berhasil masuk ke dalam grup dalam *Cloud*, akan diproses untuk sinkronisasi fitur-fitur *Cloud* yang meliputi *Remote Access*, *Log*, SSID, *Password Management*, dan fitur-fitur lainnya yang mendukung manajemen terpusat. Jika semua sudah tersinkronisasi dengan baik, selanjutnya *Cloud* memberikan IP *Egress* yang bertujuan untuk *remote management Access Point* dan sebagai jalur paket antara *Cloud* ke *Access Point*. Pada sesi ini akan muncul paket yang menunjukkan bahwa *Cloud* mengirimkan paket berupa IP *Egress* yang didaftarkan secara otomatis oleh *Cloud* untuk *Access Point*, dan informasi ini muncul di *log Bettercap* yang terdapat pada Gambar 4. IP *Egress* sendiri adalah alamat IP yang digunakan untuk proses *monitoring* dan berpotensi membatasi aliran informasi keluar dari satu jaringan ke jaringan yang lain (Sastya Hendri Wibowo, 2022). Pemahaman tentang alur data ini penting untuk mengidentifikasi titik-

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

titik kelemahan dalam komunikasi antara *Access Point* dan *Cloud*, sehingga dapat dirancang strategi mitigasi yang efektif untuk menutup celah keamanan yang ada.



Gambar 4. *Log* Paket IP *Egress*

Dengan melakukan penelitian menggunakan serangan *SSL Strip* yang termasuk dalam kategori MITM (*Man-in-the-Middle*) ini, terbukti bahwa serangan tersebut sangat mengancam keamanan data dari *Access Point* Ruijie. Ancaman yang teridentifikasi adalah penyerang dapat mengetahui *log* mulai dari *password* hingga semua data sensitif dari *Access Point* Ruijie, termasuk konfigurasi jaringan dan informasi perangkat yang terhubung. Dengan informasi ini, penyerang berpotensi mendapatkan akses tidak sah ke *device* yang terhubung ke *Access Point* tersebut, melakukan perubahan konfigurasi yang merugikan, atau bahkan menggunakan *Access Point* sebagai titik masuk untuk serangan lebih lanjut ke dalam jaringan internal organisasi. Dampak dari keberhasilan serangan ini dapat sangat merugikan, mulai dari kebocoran data sensitif, gangguan operasional jaringan, hingga potensi kerugian finansial dan reputasi bagi organisasi yang menjadi korban. Selanjutnya, untuk mengantisipasi dan memitigasi serangan dari *SSL Strip*, ada beberapa cara yang dapat diterapkan untuk meningkatkan keamanan sistem. Pertama, mengaktifkan dan memantau *log* di jaringan *Access Point* menggunakan IDS (*Intrusion Detection System*) yang dapat mendeteksi aktivitas mencurigakan secara *real-time*. Kedua, gunakan standar keamanan *wireless* yang lebih kuat seperti WPA3 atau WPA2-*Enterprise* guna menghindari penyerang dapat masuk ke jaringan dengan mudah melalui autentikasi yang lemah. Ketiga, mengaktifkan *redirect* otomatis ke HTTPS dan menerapkan HSTS (*HTTP Strict Transport Security*) pada semua layanan *web* yang diakses, sehingga *browser* akan selalu menggunakan koneksi HTTPS dan menolak koneksi HTTP yang tidak aman. Keempat, memisahkan jaringan menggunakan VLAN (*Virtual Local Area Network*) agar pengguna terisolasi satu dengan yang lain, sehingga jika satu segmen jaringan terkompromi, segmen lainnya tetap aman. Fungsi IDS adalah mendeteksi serangan seperti *brute force* dan *malware*, lalu memberikan respons kembali secara otomatis terhadap ancaman yang terdeteksi. *Firewall* dan IDS dapat memberikan keamanan berlapis dan berkolaborasi dalam menangani ancaman secara *real-time* (Sista Naelly Adzimi, September 2022). Pada penerapan keamanan, terdapat beberapa kendala yang perlu diperhatikan. Jika Ruijie mengaktifkan *wireless isolation*, yang berfungsi mencegah *device* saling berkomunikasi secara langsung di satu jaringan, hal ini dapat mengurangi risiko serangan MITM. Selain itu, mengaktifkan *Captive Portal* dengan menggunakan HTTPS dan HSTS sangat direkomendasikan karena meskipun penyerang mencoba melakukan *SSL Strip*, pengguna tetap akan diarahkan ke koneksi HTTPS yang aman, sehingga data tetap terenkripsi dan terlindungi dari intersepsi.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

4. Kesimpulan

Dengan adanya simulasi dalam penyerangan *SSL Strip*, dapat disimpulkan bahwa masih ada celah dari fitur *Cloud* yang belum maksimal dalam hal keamanan. Karena masih dapat menampilkan paket data yang akan dikirimkan dari *Access Point* ke *Cloud* berupa *Password*, SSID, IP, *Serial Number*, *Network Name*, Tipe *Device*, Versi *Firmware*, *MAC Address*, *Forward Mode*, Status *Access Point*, dan Status Port, hal ini akan mengancam hingga ke seluruh pengguna *Access Point*, khususnya data jika penyerang ingin melanjutkan serangannya. Terkait keamanan dari fitur *Cloud* ini, perlu adanya pengembangan lebih lanjut terkait keamanan yang difokuskan di perangkat *Access Point* karena masih ada celah untuk mengubah koneksi yang semula dari HTTPS menjadi HTTP. Penyerang sudah bisa melihat isi data antara *Access Point* menuju *Cloud* maupun sebaliknya, dan alangkah baiknya perlu adanya evaluasi lebih lanjut. Selain itu, batasan masalah yang dimiliki adalah keterbatasan waktu dan serangan *SSL Strip* ini memberikan hasil sesuai dengan kemampuan peneliti karena terbatas alat dan waktu. Jika pada saat implementasi serangan masih ada yang belum tercapai, bisa dilakukan bersama penguji yang lebih berkompeten.

5. Ucapan Terima Kasih

Penulis ingin menyampaikan puji syukur atas kehadirat Tuhan Yang Maha Esa atas berkat, rahmat, dan kekuatan yang telah diberikan hingga penelitian ini dapat berjalan dengan baik dan lancar. Penulis juga ingin menyampaikan rasa apresiasi dan terima kasih kepada Universitas Kristen Satya Wacana (UKSW). Ucapan terima kasih yang sebesar-besarnya juga diberikan kepada dosen pembimbing Dian W. Chandra, S.Kom., M.Cs., atas bimbingan, arahan, dan masukan sehingga penelitian ini berjalan dengan baik. Kemudian rasa hormat dan terima kasih atas fasilitas, arahan, dan dukungan selaku penunjang keberhasilan penelitian ini kepada Vinsensius Desta Venando selaku Direktur Utama PT. Data Sarana Telematika. Penghargaan yang sangat mendalam kepada orang yang saya sayangi, yaitu orang tua, karena telah memberikan dukungan penuh serta memberikan arahan selama perkuliahan dan penulisan penelitian ini. Serta kepada teman-teman yang telah memberikan dukungan secara moral maupun teknis.

6. Daftar Pustaka

Aryanto, N., & Hafid, D. A. (2024). Peranan IT security dalam mengamankan infrastruktur dan transaksi di perusahaan e-commerce. *Kohesi: Jurnal Sains dan Teknologi*, *4*(10), 13-16. https://doi.org/10.3785/kohesi.v4i10.6528.

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2022). Implementasi konfigurasi firewall dan sistem deteksi intrusi menggunakan Debian. *Public Journal of Information System Engineering*, *1*(4), 1-10. https://doi.org/10.47134/pjise.v1i4.2681

Dharmawan, N., Indriyanta, G., & Senapartha, I. K. D. (2022). Analisis Keamanan Jaringan Universitas Kristen Duta Wacana Dengan Serangan Ssl/Tls. *Jurnal Terapan Teknologi Informasi*, *6*(2), 121-130. https://doi.org/10.21460/jutei.2022.62.214

Dirgantara, R. R. C., & Suartana, I. M. (2020). Implementasi ARP watch dengan pfSense untuk mekanisme pengamanan access point. *Jurnal Manajemen Informatika*, *10*(1), 63-72.

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 7 No. 1 (2026) | Januari
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i1.1625

Faizi, M. A., & Christanto, F. W. (2024). Manajemen Perangkat Jaringan Access Point Menggunakan UniFi Controller di Jaringan Kampus. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, *9*(2), 67-76. https://doi.org/10.32528/justindo.v9i2.1471

Husein, & Gunawan, D. (2023). Penerapan Metode SNMP (Simple Network Management Protocol) dalam Optimalisasi Kinerja Jaringan Komputer Studi Kasus pada IDN Boarding School. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *4*(3), 1814-1821. https://doi.org/10.35870/jimik.v4i3.410

Hae, Y. (2021). Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *8*(4), 2095-2105. https://doi.org/10.35957/jatisi.v8i4.1196

Mallu, S., Andisana, I. P. G. S., Chyan, P., Rizki, F., Smrti, N. N. E., Syamsuddin, S., ... & Yahya, K. (2024). Sistem Operasi: Konsep Dasar dan Penerapan Modern. *Penerbit Mifandi Mandiri Digital*, *1*(01).

Martani, A. K., Munandar, A. H., & Gusman, M. A. (2023). Implementasi Global Positioning System (GPS) pada kendaraan menggunakan Mikrotik Lt AP Mini. *Jurnal Sistem Komputer*, *8*(2), 1-16. https://doi.org/10.59134/jsk.v8i2.532

Wibowo, S. H., Irawan, J. D., Wahyuddin, S., Winardi, B., Santoso, L. W., Safrizal, Yuniansyah, Dewantara, R., Jamaludin, Nurhadi, Sihombing, F. A., Aulia, A. P., Heryana, N., & Kurnaedi, D. (2022). *Cyber crime di era digital*. PT. Global Eksekutif Teknologi. https://www.academia.edu/94200419/CYBER_CRIME_DI_ERA_DIGITAL#page=28