Jurnal Sains, Teknologi dan Industri, Vol. 18, No. 2, Juni 2021, pp.188 - 195
ISSN 2407-0939 print/ISSN 2721-2041 online

Hijacking Menggunakan Metode *Man-in-the-Middle* dengan *Denial of Service* untuk memutuskan *Live Monitoring* pada UAV Untuk Pemantauan Daerah Vital

Yetti Yuniati[1], Melvi[2], Herman H Sinaga[3], Andrew[4]
[1,2,3,4] Jurusan Teknik Elektro, Fakultas Teknik, Universitas Lampung
Jl. Prof. Sumantri Brojonegoro No.1 Bandar Lampung 35145
Email: yetti.yuniati@eng.unila.ac.id

ABSTRAK

Pesatnya perkembangan *Unmaned Aerial Vehicle* (UAV) atau pesawat tanpa awak, membuat UAV memiliki banyak fungsi diantaranya, memiliki kemampuan dalam pemetaan dan pemantauan suatu daerah dengan menggunakan teknologi *open source*, dimana salah satunya adalah SiK Radio dari Ardupilot. Akan tetapi, terdapat dampak negatif UAV yang dapat dipergunakan untuk hal-hal buruk seperti pengambilan gambar berupa video pada daerah yang memiliki tingkat privasi yang tinggi seperti militer dan bandara. Dalam menjaga privasi suatu daerah, Teknik *Hijacking* merupakan salah satu pilihan untuk menjaga privasi digital. Salah satu Metode *Hijacking* yang dapat dimanfaatkan dengan tujuan utama, untuk melindungi data privasi dari pencurian adalah Metode *Man-in-the-Middle* (MITM) dengan *Denial of Service* (DoS). MITM digunakan untuk mengambil data berupa *password* keamanan dari jaringan target, sedangkan DoS untuk mengirimkan paket deautentikasi, sehingga *client* target tidak bisa menerima autentikasi dari jaringan. Pada penelitian ini telah berhasil menerapkan metode MITM dengan DoS, yang berfungsi untuk memutuskan koneksi *Live Monitoring* digital yang terintegrasi dengan UAV. Penerapan metode ini, menargetkan jaringan komunikasi *Secure Shell* (SSH) yang berada pada jaringan *Raspberry Pi* dan *device*. Sehingga, remot akses *device* ke *raspberry pi* dapat di putus dan *device* dapat diambil alih**.**

Kata kunci: UAV, *Hijacking , Man-in-the-Middle, Denial of Service, Open-Source*

ABSTRACT

The rapid development of Unmaned Aerial Vehicle (UAV) or unmanned aircraft, made UAVs have many functions, including the ability for mapping and monitoring an area using open source technology, which is SiK Radio from Ardupilot. However, there are negative impacts of UAVs which can be used for bad things such as taking video in areas, that have a high level of privacy, such as the military and airports. In maintaining the privacy of an area, the Hijacking technique is an option in maintaining digital privacy. One of the Hijacking Methods that can be a solution for the main problem, to protect privacy data from theft, is the Man-in-the-Middle (MITM) Method with Denial of Service (DoS). MITM is used to retrieve data in the form of a security password from the target network, while DoS is used to send deauthentication packets, so the target client cannot receive authentication from the network. This research has successfully implemented the MITM method with DoS, which functions to disconnect digital Live Monitoring that is integrated with UAVs. The application of this method is targeting the Secure Shell (SSH) communication network that is on the Raspberry Pi network and devices. So, remote access from the device to the raspberry can be disconnected and the device can be taken over.

Keyword: *UAV, Hijacking , Man-in-the-Middle, Denial of Service, Open-Source*

Jurnal Sains, Teknologi dan Industri, Vol. 18, No. 2, Juni 2021, pp.188 - 195
ISSN 2407-0939 print/ISSN 2721-2041 online

Pendahuluan

Perkembangan teknologi dari waktu ke waktu semakin canggih. Pada era modern ini, pemotretan udara tidak hanya dilakukan menggunakan pesawat berawak yang membutuhkan biaya yang tidak sedikit, melainkan juga menggunakan wahana pesawat tanpa awak atau UAV (*Unmanned Aerial Vehicle*). Pesawat tidak berawak terdapat dua tipe atau model UAV, yaitu *fixed wing* dan *copter* [1].

Pesawat tak berawak berbeda dengan jenis pesawat terbang lainnya. karena pada UAV didalamnya tidak terdapat pilot. Awal mula penggunaan UAV digunakan untuk perang dunia oleh angkatan militer di berbagai negara. karena kekhawatiran kehilangan pilot diatas wilayah musuh. Kini UAV sudah digunakan di berbagai bidang seperti alat pemantauan keamanan laut, pemantauan laju lalu lintas kendaraan, dan tempat *non-commercial* lainnya [2].

Penyalahgunaan fungsi UAV diantaranya, sebagai penyusup di suatu wilayah yang dilarang untuk penerbangan, serta digunakan untuk pengambilan gambar atau video secara tidak resmi. Hal ini dikarenakan beberapa teknologi *open-source* yang dikembangan oleh setiap individu. diantaranya yaitu *Ardupilot* yang menggunakan *firmware Sik Radio* [2].

Pada jenis transmisi video yang digunakan pada UAV, tidak hanya berbasis pada analog tetapi juga menggunakan transmisi digital. Peningkatan penggunaan sistem transmisi digital saat ini, karena memiliki aspek keunggulan. Salah satu aspek keunggulan yang dimiliki oleh sistem pengiriman digital adalah pada sistem keamanan WPA2-PSK, WEP, dan WPA [3].

Agar dapat mengantisipasi pengambilan data berupa video secara tidak resmi. Maka, diterapkan metode *Man-in-the-Middle (MITM)* dengan *Denial of Service (DoS)* untuk melakukan pengambilalihan terhadap wahana UAV yang digunakan oleh pelaku tersebut. Cara kerja dari metode *Man-in-the-Middle* adalah pelaku meletakkan dirinya seolah-olah ada di tengah-tengah dua perangkat yang berkomunikasi. Karna pelaku terdapat di tengah-tengah komunikasi ini, maka pelaku dapat melakukan sebuah retasan dengan memodifikasi atau pencekalan terhadap paket, yang nantinya akan dikirim atau diterima kedua perangkat tersebut. MITM bekerja dengan mengeksploitasi ARP (*Addresss Resolution Protocol*). ARP ini adalah protokol yang bertugas untuk menerjemahkan peng-alamatan dari *IP Address* menjadi suatu *MAC Address*. Serta penerapan cara kerja DoS dalam penelitian ini adalah untuk mengirimkan paket Deautentikasi, sehingga pada *client* target tidak bisa menerima autentikasi dari jaringan [5][6][10].

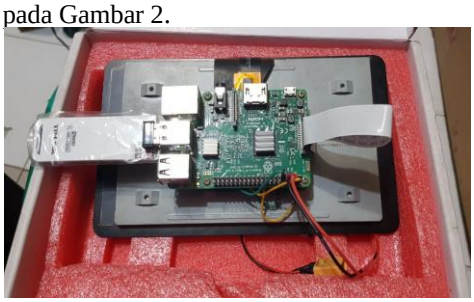
Metode Penelitian

Pembuatan *Quadrotor* sebagai target

Tahap awal yang akan dilakukan diantaranya yaitu proses pengambilan citra video melalui *Live Monitoring Device* yang berbasis transmisi digital dengan menggunakan *firmware* OPENHD yang telah terintegrasi dengan *Quadrotor* yang sudah di buat, serta beberapa komponen yang telah dipasang pada UAV jenis *rotary wing*. Pada wahana ini berisi komponen pendukung yaitu kamera *Raspberry Pi*, *Raspberry Pi* Zero, serta dongle Wi-Fi, dimana data telemetry yang diterima UAV juga di proses didalam *Raspberry Pi* zero, sehingga untuk data-data yang diperlukan dapat di tampilkan didalam OSD (*on screen display*) tampilan video tersebut. Fungsi dongle Wi-Fi adalah untuk mentransmisikan packet data yang berbasis digital yang diterima dari hasil pemrosesan *Raspberry Pi* Zero. Tampilan *Raspberry Pi* Zero yang digunakan pada penelitian ini dapat di lihat pada Gambar 1.

Gambar 1. Tampilan *Raspberry Pi Zero* dengan Kamera

Pada *Ground Control* terdapat komponen pendukung diantaranya *Raspberry Pi* 3, Wi-Fi dongle, dan LCD. Dimana setelah data ditransmisikan dari wahana dan diterima kembali di *Ground* melalui Wi-Fi dongle yang berada di *Ground*, kemudian di proses oleh *Raspberry Pi* 3, sehingga dapat diproyeksikan didalam LCD. Tampilan *Raspberry Pi* 3 yang digunakan dapat dilihat pada Gambar 2.



Gambar 2. Tampak Belakang *Raspberry Pi 3* Pada Ground

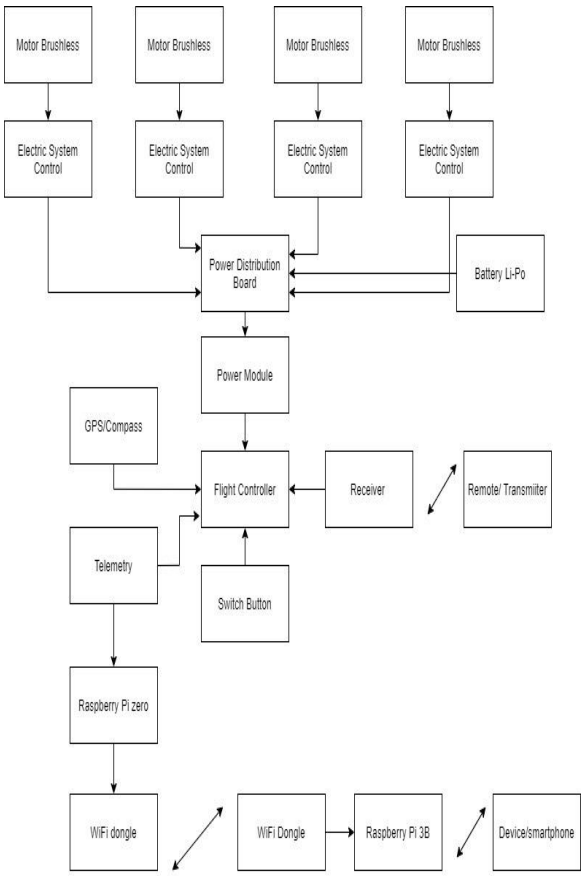
Hijacking Vulnerbility pada jaringan

Tahap kedua, komponen yang dibutuhkan untuk *Hijacking* diantaranya, *laptop (device), Wi-Fi card, OS kali Linux, Fluxion, Aircrack-ng.* Pada tahap ini, aplikasi *Fluxion* dan aplikasi *aircrack-ng* yang dijalankan didalam *OS kali linux* dipergunakan untuk mendeteksi dan memindai sinyal frekuensi

access point yang terdapat didalam daerah tersebut, *Wi-Fi card* berfungsi sebagai komponen yang mengirimkan atau meninjeksikan paket data dari laptop sehingga dapat meng-*interupt* data transmisi target. Dengan memanfaatkan beberapa fitur yang telah disebutkan diatas seperti *Fluxion* dan *aircrack-ng*, dapat dilakukan proses *Hijacking* pada target yaitu *Raspberry Pi 3* pada *Ground* akan mengaktifkan *hotspot* sebagai jembatan untuk *system control* dan pengiriman data berupa video ke penerima. Aplikasi *aircrack-ng* akan memindai serta mengirimkan paket *deauthication* melalui *Wi-Fi card* yang telah terintegrasi dengan laptop, sehingga *device* yang terkoneksi dengan *raspberry* tersebut tidak dapat melalukan authentikasi dan kemudian terputus. Dengan konsep *Denial of Service*, maka paket akan di kirimkan secara terus menerus. Kemudian untuk mendapatkan *password*/keamanan WPA-2/WPA pada *hotspot* tersebut, di manfaatkan fitur *Man-in-the-Middle*, dimana ketika *user* ingin melakukan *reconnecting* dan memasukan *password access point* yang terdapat pada *raspberry*, maka kita akan mendapatkan *password* tersebut melalui fitur *Fluxion*.

Desain Perangkat Keras (*Hardware)*

Pada Gambar 3. Menjelaskan tentang diagram blok perangkat keras pada *Quadrotor*.



Gambar 3. Blok diagram perangkat keras *Quadrotor*

Komponen perangkat keras yang digunakan untuk pengambilan data berupa *mounting* atau dudukan kamera yang dibuat menggunakan *additive manufacturing* atau lebih dikenal sebagai *3D printing* dengan bahan plastik PLA. Dudukan kamera ini didesain sedemikian rupa untuk menempatkan kamera agar memiliki sudut pandang yang luas dan tidak terhalangi oleh apapun.

Gambar 4. *Quadrotor* yang terpasang kamera

Skema Proses Penerapan Pembajakan

Pada *Air*:

Pada Gambar 5, terdapat tahapan awal yang akan dilakukan diantaranya yaitu dalam pengambilan citra video melalui *Live Monitoring Device* yang berbasis transmisi digital dengan menggunakan firmware OPENHD yang telah terintegrasi dengan *Quadrotor* yang sudah di buat dan beberapa komponen yang telah dipasang pada UAV jenis rotary wing. Pada wahana ini berisi komponen pendukung yaitu kamera *Raspberry Pi*, *Raspberry Pi* Zero ,serta dongle Wi-Fi, dimana data telemetry yang diterima UAV juga di proses didalam *Raspberry Pi* zero sehingga untuk data-data yang diperlukan dapat di tampilkan didalam OSD(On Screen Display) tampilan video tersebut, dan fungsi dongle Wi-Fi tersebut untuk mentransmisikan packet data yang berbasis digital yang diterima dari hasil pemrosesan *Raspberry Pi* Zero tersebut.

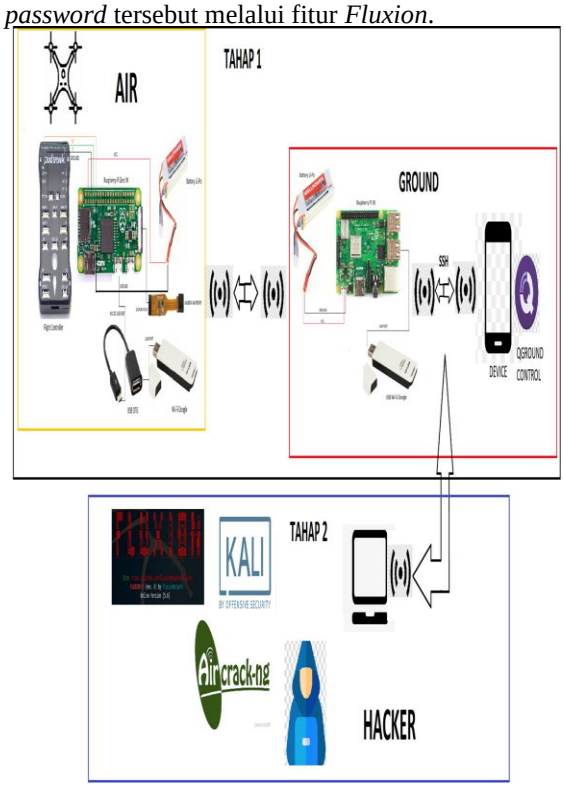
Pada *Ground*:

Pada *Ground* Control yang ditunjukkan oleh Gambar 5, terdapat komponen pendukung diantaranya *Raspberry Pi* 3, Wi-Fi dongle, dan LCD, dimana setelah data ditransmisikan dari wahana dan diterima kembali di *Ground* melalui Wi-Fi dongle yang berada di *Ground*, kemudian di proses oleh *Raspberry Pi* 3 sehingga dapat diproses datanya untuk digunakan dalam aplikasi Q*Ground* Control yang telah terinstall pada *device*. Jenis koneksi yang digunakan dalam berkomunikasi antara *Raspberry Pi* 3 dan *smartphone* adalah *Secure Shell* (SSH).

Jurnal Sains, Teknologi dan Industri, Vol. 18, No. 2, Juni 2021, pp.188 - 195
ISSN 2407-0939 print/ISSN 2721-2041 online

Pada Pelaku pembajakan:

Pada Gambar 5 bagian tahap kedua, komponen yang dibutuhkan untuk *Hijacking* diantaranya, laptop (*Device*), Wi-Fi *card*, OS kali Linux, *Fluxion*, *Air*crack-ng. pada tahap ini, aplikasi *Fluxion* dan aplikasi *air*crack-ng yang dijalankan didalam OS kali linux dipergunakan untuk mendeteksi dan memindai sinyal frekuensi access point yang terdapat didalam daerah tersebut. Wi-Fi *card* berfungsi sebagai komponen yang mengirimkan atau meninjeksikan paket data dari laptop sehingga dapat meng-*interupt* data transmisi target. Dengan memanfaatkan beberapa fitur yang telah disebutkan diatas seperti *Fluxion* dan *air*crack-ng, dapat dilakukan proses *Hijacking* yang dimana pada target yaitu *Raspberry Pi* 3 pada *Ground* akan mengaktifkan hotspot sebagai jembatan untuk system control dan pengiriman data berupa video ke penerima. Aplikasi *air*crack-ng akan memindai serta mengirimkan paket *deauthication* melalui Wi-Fi *card* yang telah terintegrasi dengan laptop, sehingga *device* yang terkoneksi dengan Raspberry tersebut tidak dapat melalukan authentikasi dan kemudian terputus. Dengan konsep *Denial of Service*, maka paket akan dikirimkan secara terus menerus. Kemudian untuk mendapatkan *password*/keamanan WPA-2/WPA pada hotspot tersebut, di manfaatkan fitur Man in the middle, dimana ketika *user* ingin melakukan *reconnecting* dan memasukan *password access point* yang terdapat pada Raspberry, maka akan didapatkan *password* tersebut melalui fitur *Fluxion*.

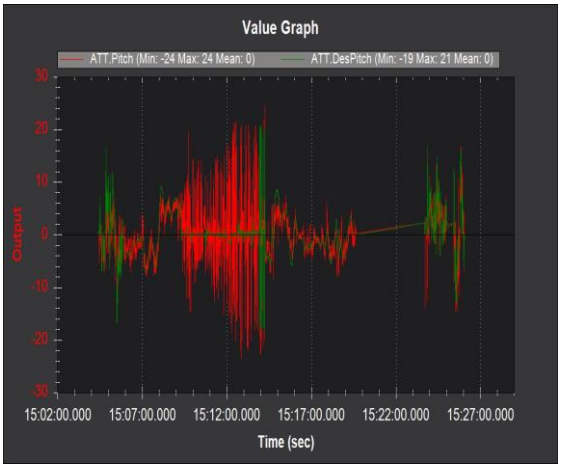


Gambar 5. Skema Proses Penerapan Pembajakan

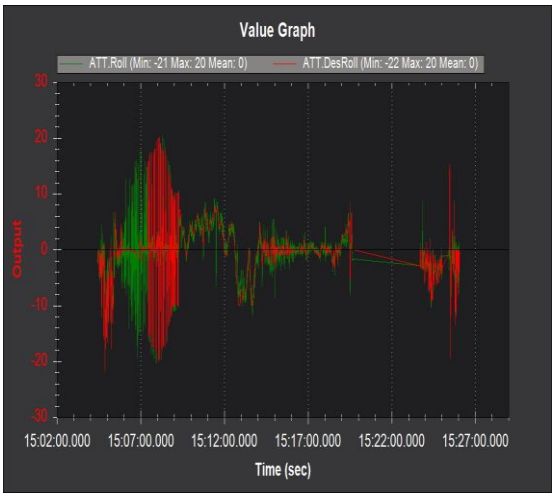
Hasil dan Pembahasan

Hasil Respon Setelah Autotune

Pada tahap pengambilan data uji untuk stabilitas *Quadrotor*, maka dilakukan uji terbang *autonomous Tuning* pada wahana sehingga mendapatkan respon yang bagus untuk menghasilkan tampilan HUD yang stabil. Pada Gambar 6 merupakan gambaran respon *pitch*. Fungsi dari *pitch* untuk mengatur respon maju dan mundur dari tampak depan *Quadrotor*. Grafik respon setelah melakukan *tuning* dan respon yang diharapkan memiliki perbedaan dikarenakan pada saat tuning terjadi gangguan yang tidak diinginkan diantaranya interferensi angin sinyal dan lainnya, Gambar 7. Menunjukkan grafik respon *roll*, yang berfungsi sebagai respon untuk belok kanan dan kiri. Pada grafik respon yang diharapkan dan realita setelah melakukan tuning terlihat pada gambar tersebut, grafik respon *roll* memiliki sedikit respon yang serupa dengan yang di harapkan. Pada Gambar 8 menunjukkan grafik respon *yaw* yang berfungsi sebagai respon belok kanan dan kiri. Berbeda dengan respon *roll*, respon *yaw* akan membuat *Quadrotor* menghadap kekanan dan kekiri sesuai dengan perintah yang diberikan. Pada respon *yaw* terlihat sangat baik dikarenakan respon yang diharapkan dan respon setelah *tuning* memiliki grafik yang sama.



Gambar 6. Grafik Respon *Pitch*

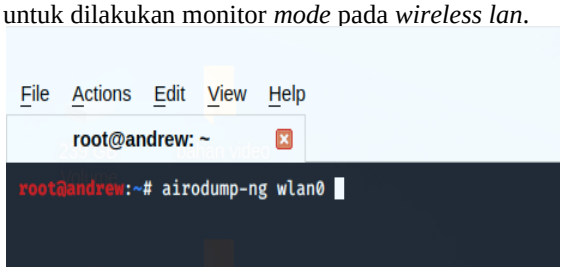


Gambar 7. Grafik Respon R*oll*

Gambar 8. Grafik Respon Y*aw*

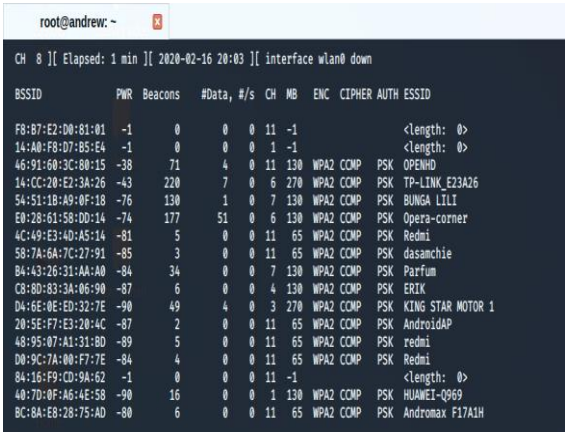
Hasil Penerapan Metode *Denial of Service*

Tahap awal adalah membuka aplikasi airodump dan menggunakan *device* yang tersedia untuk dilakukan monitor *mode* pada *wireless lan*.



Gambar 9. Screenshoot Airodump-ng wlan0

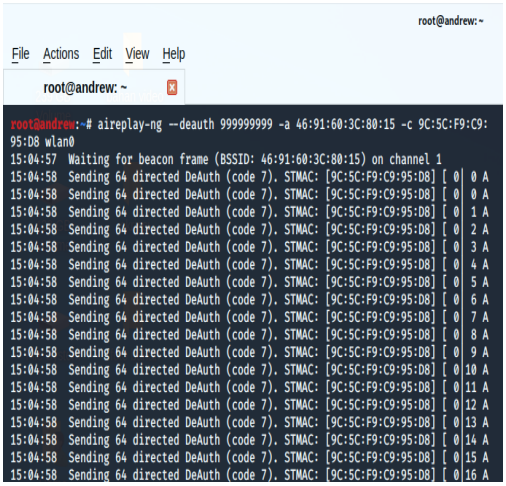
Setelah membuka *airodump*, maka akan muncul jaringan yang tersedia pada lingkungan sekitar *wireless lan* yang terdeteksi. Tampilan beberapa jaringan yang terdeteksi dapat dilihat pada Gambar 10.



Gambar 10. Jaringan yang Terdeteksi

Jika terdapat *Mac Address* jaringan asing muncul, maka dapat dilihat didalam jaringan tersebut berapa banyak *device* yang terkoneksi pada *access point* tersebut. Untuk mengeluarkan *user* yang terkoneksi dengan suatu jaringan secara paksa, dapat dilakukan dengan mengirimkan paket deauthentikasi agar *device* tersebut tidak bisa menerima autentikasi dari jaringannya.

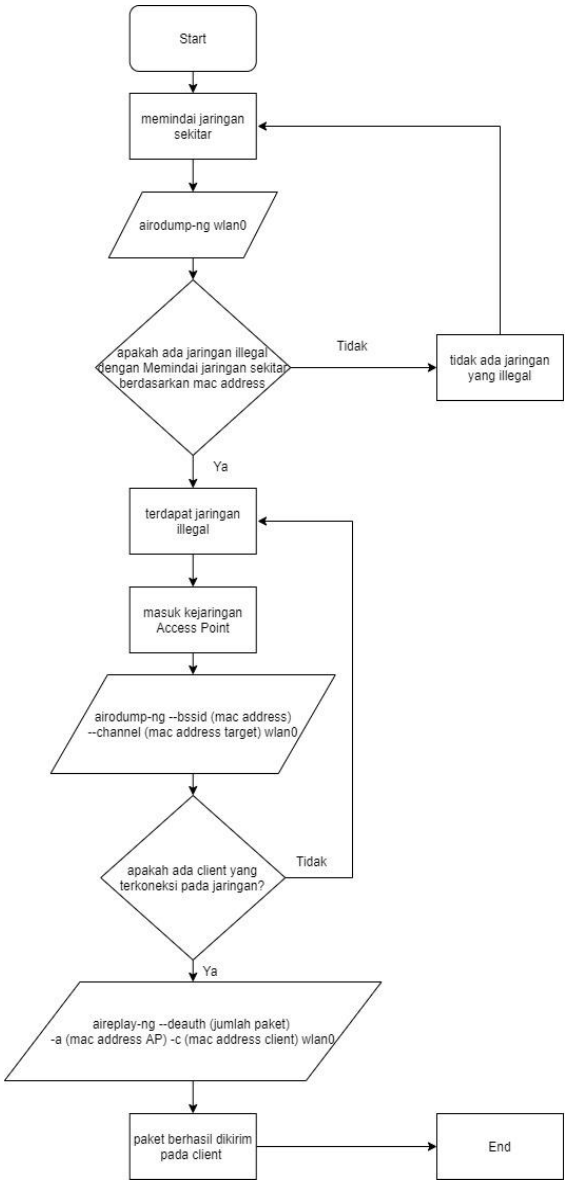
Gambar 11. *Command* untuk Mengirimkan *deauthication packets* pada Jaringan



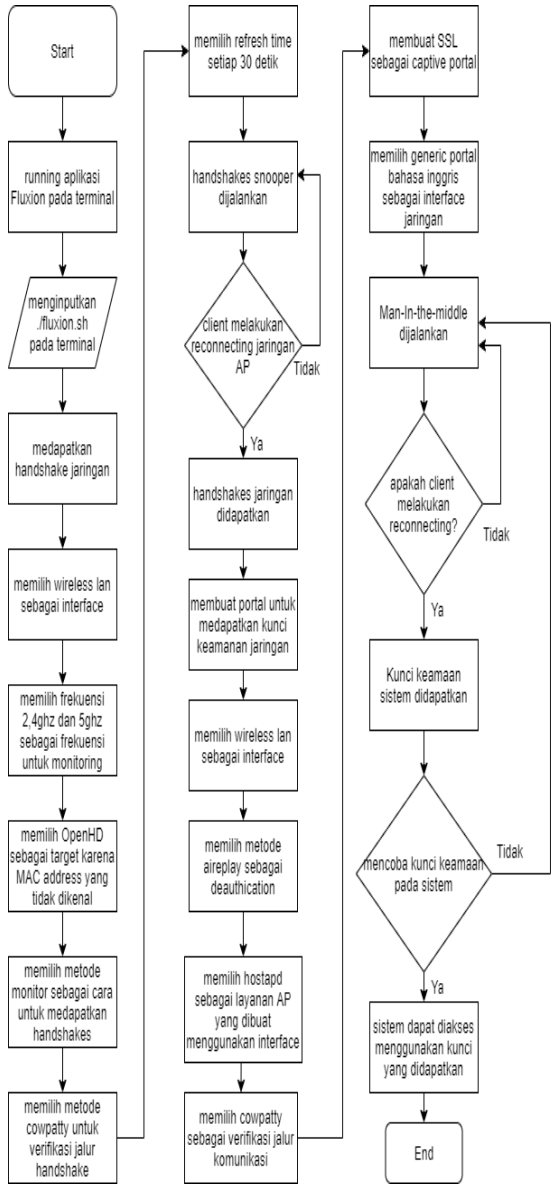
Gambar 12. Informasi Paket yang sedang dikirim

Proses penerapan *Denial of Service* dapat di lihat pada Gambar 13.

Jurnal Sains, Teknologi dan Industri, Vol. 18, No. 2, Juni 2021, pp.188 - 195
ISSN 2407-0939 print/ISSN 2721-2041 online



Gambar 13. Proses *Denial of Service*

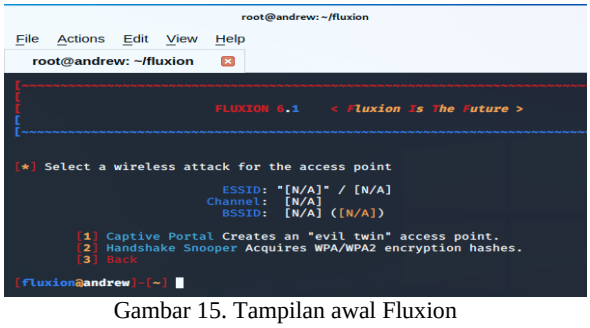


Gambar 14. Proses *Man-In-The-Middle*

Hasil Penerapan Metode Man-in-the-Middle

Proses penerapan metode MITM dapat dilihat pada Gambar 14. Pada bagian ini, untuk proses mendapatkan data dari pelaku. Maka, digunakan *Fluxion* untuk mengambil data berupa *password* keamanan dari jaringan target. Tampilan awal Fluxion dapat dilihat pada Gambar 15.

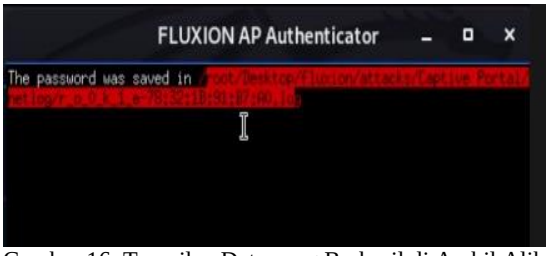
Pada Gambar 14 menjelaskan diagram alir proses peretasan yang dimulai dari memindai jaringan target.



Gambar 15. Tampilan awal Fluxion

Kemudian untuk mendapatkan kunci *handshake* diperoleh dengan cara memutus semua *client* yang terkoneksi pada jaringan target, agar *client* yang terputus dan berusaha kembali untuk memasuki jaringan tersebut. Jaringan target akan menginsialkan bahwa jaringan peretas merupakan

jaringan yang sama dengan *client* target yang ingin memasuki ulang jaringannya. Ketika sudah mendapatkan *handshake*, maka langkah selanjutnya adalah membuat jaringan palsu yang memiliki spesifikasi seperti jaringan asli. Ketika jaringan palsu telah di buat, maka *client* tidak bisa membedakan jaringan asli/palsu dan tidak bisa memasuki jaringan asli, dikarenakan jaringan asli telah mendapatkan paket *flooding* melalui *Denial of Service*. Jika terdapat c*lient* yang ingin memasuki jaringan tersebut, maka tidak akan menerima autentikasi dari jaringan yang dituju. Pada jaringan palsu, ketika *client* memasuki jaringan tersebut dan menginputkan *password* keamanan jaringan dengan benar, maka pada peretas akan mendapatkan kunci tersebut secara otomatis.



Gambar 16. Tampilan Data yang Berhasil di Ambil Alih

Tingkat keberhasilan dari proses hijacking ini tergantung dari pihak *user* yang harus melakukan *reconnecting* dan *handshake* jaringan *user* didapatkan. Jika kedua proses ini dilakukan, maka proses hijacking akan sukses.

Kesimpulan

Setelah dilakukan penelitian dan pembahasan maka dapat diambil simpulan bahwa pada penelitian ini telah berhasil menerapkan metode *Man-in-the-Middle* dengan *Denial of Service* untuk memutuskan sistem transmisi video berbasis digital pada wahana *Quadrotor*. Pada proses untuk mendapatkan *handshake* jaringan transmisi video, dibutuhkan koneksi ulang dari *user* target terhadap jaringan tersebut. Dikarenakan, pada jaringan SSH yang dituju, *user* akan menidentifikasi bahwa jaringan yang ingin terkoneksi pada jaringan tersebut adalah *user* target. Pada perangkat keras yang digunakan untuk mendukung sistem transmisi memiliki kelemahan diantaranya pada daya proses transmisi video dari Tx dan Rx yang berpengaruh pada kualitas video yang di terima dari pemancar, karena pada WDN3200 memiliki daya <100mW dan bekerja pada frekuensi 5,8Ghz yang mengakibatkan sinyal rentan terkena inteferensi dari kuat sinyal lainnya yang bekerja pada frekuensi 5,8Ghz.

Daftar Pustaka

[1] Ventura, D., Bonifazi, A., Gravina, M. F., Belluscio, A., & Ardizzone, G. (2018). *Mapping and classification of ecologically sensitive marine habitats using unmanned aerial vehicle (UAV) imagery and object-based image analysis (OBIA). Remote Sensing*, 10(9), 1331.

[2] Abdullah, M, 2019. Tanggung Jawab Komando Atas Penyalahgunaan Umanned Aerial Vehicle Jenis Drone Dalam Hukum Humaniter Internasional. ETD Unsyiah.

[3] Purwanto, T. D., & Wijaya, A. (2017). Evaluasi Aplikasi Exploid Wifi Di Tingkat *Availability Dan Vulnerability.* Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 8(2), 801-806.

[4] Santoso, M. R., Wahyudi, W., & Sudjadi, S. (2019). simulasi kontrol *roll, pitch* dan *yaw* pada *quadrotor* menggunakan PID dan LQR. Transient: Jurnal Ilmiah Teknik Elektro, 7(2), 686-693.

[5] Song, Y. (2017). U.S. Patent No. 9,667,541. Washington, DC: U.S. Patent and Trademark Office.

[6] Biron, Z. A., Dey, S., & Pisu, P. (2018). *Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Transactions on Intelligent Transportation Systems*, 19(12), 3893-3902.

[7] Zhang, P., Wang, H., Hu, C., & Lin, C. (2016). *On denial of service attacks in software defined networks. IEEE Network*, 30(6), 28-33.

[8] WIss, V. G. (2020). *Facilitating Frame Injection Exploits through SiK Radio Firmware Modification (Doctoral dissertation, Christopher Newport University)*.

[9] Sherman, A. T., Seymour, J., Kore, A., & Newton, W. (2017). *Chaum's protocol for detecting man-in-the-middle: Explanation, demonstration, and timing studies for a text messaging scenario.* Cryptologia, 41(1), 29-54.

[10] Breński, K., Chołuj, M., & Luckner, M. (2017, June). *Evil-AP-Mobile Man-in-the-Middle Threat. In IFIP International Conference on Computer Information Systems and Industrial Management* (pp. 617-627). Springer, Cham.

[11] Adams, K. (2019). U.S. Patent No. 10,171,250. Washington, DC: U.S. Patent and Trademark Office.

[12] Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). *Man-in-the-middle attack in wireless and computer networking—A review. In 2017 3rd International Conference on Advances in Computing, Communication & Automation* (ICACCA)(Fall) (pp. 1-6). IEEE.

[13] Wang, H., Xu, L. and Gu, G., 2015, June. *Floodguard: A dos attack prevention extension in software-defined networks. In 2015 45th Annual IEEE/IFIP International Conference*

on Dependable Systems and Networks (pp. 239-250).

[14] Süzen, A. A., Duman, B., & Şen, B. (2020, June). *Benchmark Analysis of Jetson TX2, Jetson Nano and Raspberry PI using Deep-CNN. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications* (HORA) (pp. 1-5). IEEE.

[15] Hsu, F. H., Hwang, Y. L., Tsai, C. Y., Cai, W. T., Lee, C. H., & Chang, K. (2016). TRAP: A *three-way handshake server for TCP connection establishment. Applied Sciences*, 6(11), 358.

[16] Yi, Y., & Gong, G. (2019). *Implementation of three LWC Schemes in the WiFi 4-Way Handshake with Software Defined Radio*. arXiv preprintarXiv:1909.11707.