SAIN TEKOM
ISSN 2088-1770 (Print)
ISSN 2503-3247 (Online)
Vol. 15 No.2 (2025) 165-176

JURNAL
SAINTEKOM
Sains, Teknologi, Komputer, dan Manajemen

Analisis Trafik Jaringan menggunakan Wireshark untuk Deteksi Serangan Deauthentication pada Perangkat Kamera Wi-Fi

*Anisa Febriyana Putri[1], Abdul Hadi[2], Lili Rusdiana[3]
[1,2,3)]Teknik Informatika, STMIK Palangkaraya
Jl. G. Obos No. 114, Palangka Raya, Kalimantan Tengah
Email: [1]riverflowsaway@gmail.com, [2]abdulhadi@stmikplk.ac.id, [3]fasliiana7@gmail.com

ABSTRACT

The widespread adoption of wireless networks has increased the popularity of Wi-Fi-based cameras due to their ease of installation and flexibility. However, Wi-Fi devices are highly vulnerable to deauthentication attacks, a type of denial-of-service (DoS) attack that repeatedly disconnects devices from the network without user awareness. This study presents a controlled experiment simulating deauthentication attacks on Wi-Fi cameras and detecting them using Wireshark. The findings demonstrate that these attacks consistently disrupt camera connectivity, causing interruptions of 50 seconds to 1 minute and 18 seconds across two scenarios. In the first scenario, the camera connection temporarily recovered between disruptions, while in the second, it remained in a reconnecting state without restoration. All attacks were successfully identified through captured deauthentication packets. This work provides experimental validation of a widely used deauthentication attack technique leveraging the Kali Linux operating system, emphasizing its significant impact on Wi-Fi cameras. Furthermore, it highlights the importance of developing mitigation strategies to address this threat in real-world environments.

Keywords : wi-fi camera; deauthentication attack; network security

ABSTRAK

Perkembangan jaringan nirkabel mendorong popularitas penggunaan kamera berbasis Wi-Fi karena kemudahan instalasi serta fleksibilitas penggunaannya. Namun, perangkat berbasis Wi-Fi dinilai cukup rentan terhadap serangan *deauthentication*, salah satu jenis serangan *denial-of-service* (DoS) yang memutus koneksi perangkat dari jaringan secara berulang tanpa sepengetahuan pengguna. Penelitian ini melakukan simulasi serangan *deauthentication* terhadap kamera Wi-Fi dan mendeteksinya menggunakan Wireshark dengan pendekatan eksperimen terkontrol. Hasil pengujian menunjukkan bahwa serangan ini secara konsisten memutus koneksi kamera dengan durasi gangguan berkisar antara 50 detik hingga 1 menit 18 detik dalam dua skenario simulasi berbeda. Pada simulasi pertama, koneksi kamera mengalami fase normal di antara gangguan, sedangkan pada simulasi kedua, kamera tetap dalam kondisi *reconnecting* tanpa pemulihan. Semua serangan berhasil terdeteksi melalui tangkapan paket *deauthentication* menggunakan Wireshark. Penelitian ini menyoroti metode serangan *deauthentication* yang umum terjadi dengan memanfaatkan sistem operasi Kali Linux, bukti eksperimental mengenai dampaknya yang signifikan terhadap kamera Wi-Fi, serta peluang pengembangan strategi mitigasi untuk mencegah serangan serupa di skenario nyata.

Kata kunci : kamera wi-fi; *deauthentication attack*; keamanan jaringan

Diterima Redaksi: 13-8-2025 | Selesai Revisi: 14-9-2025 | Diterbitkan Online: 30-9-2025

1. PENDAHULUAN

Perkembangan teknologi jaringan nirkabel telah memberikan kemudahan dalam akses komunikasi dan transfer data secara efisien antar perangkat. Salah satu perangkat yang mengadopsi penerapan teknologi ini adalah kamera Wi-Fi. Teknologi ini telah digunakan di berbagai sektor, mulai dari pengawasan keamanan rumah pribadi hingga pemantauan fasilitas publik. Kemudahan proses instalasi tanpa memerlukan kabel jaringan yang rumit menjadikan kamera Wi-Fi sebagai pilihan utama dalam sistem pengawasan modern. Namun, di balik kemudahan tersebut, kamera Wi-Fi sebagai salah satu perangkat berbasis koneksi IP juga tergolong cukup rentan terhadap serangan siber (Gustafsson & Kvist, 2022), khususnya serangan *deauthentication* yang merupakan salah satu jenis serangan yang paling umum terjadi pada jaringan Wi-Fi (Korolkov et al., 2021).

Serangan *deauthentication* merupakan bagian dari serangan *denial-of-service* (DoS) yang memanfaatkan celah pada proses autentikasi jaringan Wi-Fi. Dalam serangan ini, penyerang mengirimkan paket *deauthentication* palsu ke perangkat yang terhubung, menyebabkan perangkat tersebut terputus dari jaringan dan harus melakukan autentikasi ulang. Serangan dapat dilakukan berulang kali sehingga perangkat yang menjadi target, seperti kamera Wi-Fi yang bergantung pada koneksi stabil akan terus terputus dari jaringannya (Rakhra et al., 2020). Serangan ini bisa menjadi sangat berbahaya karena ketika kamera Wi-Fi terus terputus dari jaringan, sistem pengawasan tidak dapat memantau dan merekam aktivitas di tempat yang menjadi objek secara efektif tanpa sepengetahuan pengguna (Valente et al., 2019).

Untuk mengatasi ancaman tersebut, diperlukan solusi untuk dapat mendeteksi serangan *deauthentication* secara *real-time*. Wireshark, sebuah perangkat lunak *open-source* untuk analisis jaringan menjadi salah satu alat yang dinilai efektif untuk mengidentifikasi adanya serangan ini. Wireshark bekerja dengan menangkap dan menganalisis lalu lintas jaringan secara rinci, termasuk mendeteksi paket *deauthentication* yang mencurigakan (Korolkov et al., 2021). Fungsi ini memungkinkan administrator jaringan atau peneliti keamanan untuk memantau

DOI: https://doi.org/10.33020/saintekom.v15i2.967

anomali yang dapat menunjukkan adanya kecenderungan serangan *deauthentication*.

Sebuah studi yang dilakukan oleh Sharma dan Mittal (2019) telah mencoba menelaah mekanisme serangan *deauthentication* pada tiga perangkat komputer berbasis WLAN yang disimulasikan sebagai *access point, victim,* dan *attacker*. Hasil penelitian menunjukkan bahwa *packets* yang dikirimkan AP selama simulasi serangan berlangsung mengalami *loss*. Sementara paket TCP yang diterima *victim* terus berkurang seiring meningkatnya paket *deauthentication* yang dikirim oleh *attacker* untuk menginterupsi komunikasi antara AP dan *victim*. *Tool* analisis jaringan Wireshark juga digunakan dalam mekanisme simulasi pada penelitian ini. Meskipun pemetaan anomali paket dan simulasi sudah berhasil dilakukan pada studi ini, pendekatan yang dilakukan masih terbatas pada lingkungan simulasi pada perangkat komputer yang terhubung ke jaringan WLAN dan belum mencakup perangkat *Internet of Things* (IoT) seperti kamera Wi-Fi, yang dampaknya mungkin bisa lebih luas karena melibatkan aktivitas manusia secara nyata dan lebih dekat sehingga dapat menyentuh aspek pelanggaran privasi hingga potensi kejahatan.

Penelitian yang dilakukan oleh Gustavsson dan Kivst (2022), melangkah lebih jauh dengan menguji keamanan pada 2 sampel kamera Wi-Fi dengan metode *penetration testing*. Penelitian ini menemukan celah keamanan pada konfigurasi kamera yang dapat menimbulkan akses tidak sah dari pihak ketiga ketika informasi *root login* bocor. Temuan ini lebih menggarisbawahi kerentanan dari sisi perangkat kamera Wi-Fi, namun belum mengusulkan mekanisme deteksi dari serangan *deauthentication* secara *real-time*. Ancaman serangan ini juga dapat menjadi potensi bagi perangkat kamera Wi-Fi bahkan ketika penyerang belum memiliki informasi apapun terkait konfigurasi kamera dan jaringan nirkabel.

Penelitian yang dilakukan oleh Gopal, Prasanth, Krishna, dan Kumar (2020) membahas eksperimen serangan *deauthentication* pada perangkat *drone* dan kamera yang beroperasi berbasis jaringan nirkabel. Serangan diluncurkan melalui mikrokontroler ESP8266 yang

DOI: https://doi.org/10.33020/saintekom.v15i2.967

diprogram melalui Arduino IDE dan berhasil menyerang kedua perangkat target yang ditandai dengan terputusnya koneksi *drone* dan kamera IP tersebut. Mekanisme simulasi serangan pada penelitian ini dilakukan dengan mikrokontroler ESP8266 dan belum mencakup serangan yang diluncurkan melalui *tools* yang bekerja di sistem operasi Kali Linux. Mekanisme ini umumnya lebih sering ditemukan pada kasus-kasus serangan siber sehingga lebih berpotensi untuk dapat menyerang keamanan kinerja perangkat berbasis IoT seperti kamera Wi-Fi.

Berdasarkan uraian studi-studi di atas, dapat diidentifikasi adanya kesenjangan penelitian terkait evaluasi dampak serangan *deauthentication* terhadap perangkat IoT, khususnya kamera Wi-Fi, dengan teknik serangan yang mencerminkan skenario dunia nyata. Penelitian sebelumnya belum secara komprehensif menguji dampak serangan terhadap konektivitas kamera Wi-Fi sebagai perangkat berbasis IoT maupun mendemonstrasikan deteksi serangan secara langsung di lingkungan berbasis Kali Linux. Penelitian ini berkontribusi dengan mengisi celah tersebut melalui eksperimen terkontrol yang menyoroti dampak signifikan serangan *deauthentication* terhadap kamera Wi-Fi serta membuka peluang pengembangan strategi mitigasi yang lebih aplikatif.

2. METODE

2.1. Tinjauan Umum

Penelitian ini berfokus pada simulasi serangan *deauthentication* pada perangkat kamera Wi-Fi dan analisis terhadap keberhasilan serangan tersebut melalui penggunaan aplikasi Wireshark. Dalam penelitian ini, serangan dilakukan dengan memanfaatkan *tools* aireplay-ng yang dijalankan di atas sistem operasi Kali Linux serta Wireshark yang digunakan untuk mendeteksi dan mencatat aktivitas trafik jaringan terkait dengan simulasi serangan tersebut.

Tujuan utama dari penelitian ini adalah untuk melihat eksekusi serangan *deauthentication* pada kamera Wi-Fi dan terdokumentasinya oleh Wireshark melalui penangkapan *deauthentication packets* yang dikirim selama serangan berlangsung. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam memahami kerentanan kamera Wi-Fi terhadap serangan jaringan serta kemampuan alat

DOI: https://doi.org/10.33020/saintekom.v15i2.967

monitoring jaringan dalam mendeteksi jenis serangan ini.

2.2. Alur Penelitian

Pada penelitian ini, serangan *deauthentication* akan disimulasikan pada lingkungan terkontrol dan menganalisis dampaknya pada koneksi kamera Wi-Fi. Setiap pengukuran yang diperoleh selama simulasi serangan akan didokumentasikan dan dianalisis menggunakan Wireshark. Beberapa tahapan dalam penelitian ini, yaitu :

a. Observasi, peneliti melakukan pengamatan awal terhadap kondisi sistem jaringan untuk memastikan kamera Wi-Fi berfungsi dengan baik dan terhubung secara stabil ke jaringan.

b. Pengaturan Jaringan Wi-Fi, kamera dihubungkan ke *access point* dengan jaringan yang stabil sebelum serangan dilakukan.

c. Simulasi Serangan, tahap ini diawali dengan mengidentifikasi target dengan *tools* airodump-ng untuk menemukan informasi terkait kamera Wi-Fi dan *access point* yang menjadi target. Wireshark juga mulai diaktifkan sebelum serangan diluncurkan untuk menangkap dokumentasi trafik jaringan secara akurat. Kemudian, dilanjutkan dengan peluncuran serangan dalam dua tahap menggunakan aireplay-ng yang ditujukan pada *access point* pada tahap pertama dan kamera Wi-Fi pada tahap kedua.

Pemilihan perangkat dan lingkungan uji dilakukan untuk merepresentasikan skenario dunia nyata dalam penggunaan kamera Wi-Fi berbasis IoT. Kamera Wi-Fi kelas konsumen dengan konfigurasi standar dipilih karena umum digunakan di rumah tangga maupun kantor skala kecil, sehingga hasil pengujian relevan dengan kondisi pengguna. *Access point* standar rumah tangga digunakan untuk mensimulasikan jaringan WLAN dengan pengaturan default, sedangkan laptop simulasi penyerang dengan Kali Linux dipilih karena sistem operasi ini banyak digunakan untuk pengujian penetrasi dan umum dijumpai dalam praktik serangan siber. Pengujian dilakukan di lingkungan non-laboratorium dengan jarak perangkat sekitar 3 meter untuk meminimalkan interferensi sinyal sekaligus mempertahankan kondisi realistis.

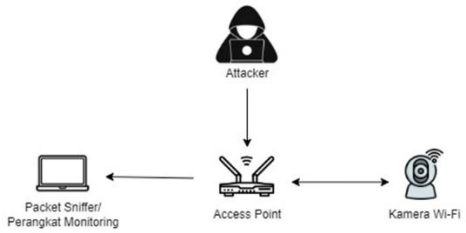
DOI: https://doi.org/10.33020/saintekom.v15i2.967

Tabel 1. *Software* dan *Hardware* Pendukung

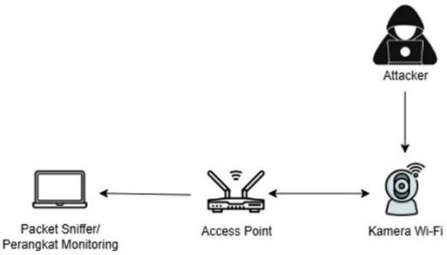
Alat	Spesifikasi/Deskripsi
Kamera Wi-Fi	V380 Pro, terhubung ke jaringan Wi-Fi untuk diuji selama simulasi serangan
Laptop	Lenovo Ideapad Slim 3i (14", 8), prosesor Intel i5, RAM 8GB, penyimpanan 256GB
Access Point Wi-Fi	ZTE F609
Adaptor Wi-Fi	TP-Link TL-WN722N Versi 1
Kali Linux V2024.2	Sistem operasi berbasis Linux untuk keamanan siber, dijalankan di atas mesin virtual (VM)
VirtualBox V7.0.12	Perangkat lunak virtualisasi untuk menjalankan Kali Linux
Aireplay V1.7	Perangkat lunak bagian dari rangkaian *tools* Aircrack-ng suite. Digunakan untuk meluncurkan paket-paket *deauthentication* pada target.
Wireshark V4.4.0	Perangkat lunak analisis paket jaringan.

2.3. Desain Simulasi Serangan

Proses terjadinya serangan diilustrasikan dengan adanya pihak ketiga selaku *attacker* yang mengganggu koneksi kamera dan AP, bersama dengan perangkat *monitoring* yang memantau berlangsungnya situasi tersebut. Simulasi dilakukan dalam dua tahap, yaitu simulasi pertama dengan menargetkan *access point* yang terhubung pada kamera, serta simulasi kedua yang akan diluncurkan dengan perangkat kamera langsung sebagai target utamanya. Berikut Gambar 1 dan 2, desain untuk memahami proses serangan secara keseluruhan dan memberikan gambaran jelas mengenai cara kerja serangan.



Gambar 1. Desain Simulasi Serangan I



Gambar 2. Desain Simulasi Serangan II

3. HASIL DAN PEMBAHASAN

Simulasi serangan dilakukan dalam dua tahap; simulasi pertama dilakukan dengan metode *broadcast* yang menargetkan *access point* yang terhubung pada perangkat kamera, kemudian simulasi kedua diluncurkan dengan menargetkan langsung pada perangkat kamera.

Proses implementasi diawali dengan pengaturan jaringan untuk memastikan kamera terhubung pada

DOI: https://doi.org/10.33020/saintekom.v15i2.967

jaringan yang stabil serta memastikan perangkat adaptor Wi-Fi terhubung dan berfungsi dengan baik. Pengecekan koneksi kamera dilakukan dengan memantau hasil *live viewing* kamera melalui aplikasi pemantauan secara *real-time*.

3.1. Simulasi Serangan I

Proses simulasi ini dilakukan dengan menjadikan *access point* sebagai target utama serangan. Paket *deauthentication* dikirimkan secara *broadcast* pada seluruh perangkat yang terhubung pada *access point*, sehingga serangan ini juga berpotensi untuk mengganggu koneksi perangkat selain target utama (kamera) yang juga terhubung ke *access point*.

Simulasi serangan diawali dengan pemindaian jaringan dengan *tools* airodump-ng untuk memperoleh informasi SSID dari perangkat *access point* target, dilanjutkan dengan penguncian adaptor pada *channel* target dan peluncuran serangan. Serangan mulai diluncurkan pada pukul 00.34 WIB yang berlangsung selama 3 menit.

3.2. Simulasi Serangan II

Pada simulasi ini, target utama ditetapkan langsung pada perangkat kamera Wi-Fi dengan mengirimkan paket *deauthentication* secara spesifik pada kamera. Proses ini dipastikan tidak akan mengganggu lalu lintas jaringan lain selain antar dua perangkat target (*access point* dan kamera) sehingga serangan dapat diluncurkan secara terarah dengan target yang spesifik.

Seperti simulasi pertama, peluncuran simulasi kedua juga diawali dengan pemindaian jaringan di sekitar. proses *scanning* dilakukan setelah penguncian adaptor pada *channel access point* untuk mempermudah pencarian SSID target. Target pada simulasi kedua merupakan perangkat kamera Wi-Fi yang sudah terhubung dengan *access point* sebagai klien, sehingga pemindaian bisa difokuskan hanya pada perangkat-perangkat yang sedang aktif melakukan komunikasi dengan *access point*. Setelah perangkat target berhasil dideteksi, serangan kedua mulai diluncurkan pada pukul 23.21 WIB yang berlangsung selama 1 menit dan 3 detik.

3.3. Pembahasan

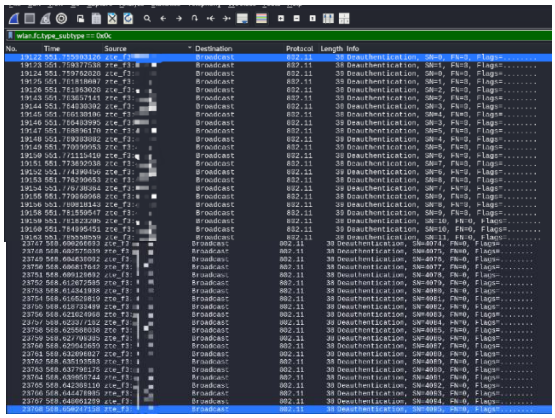
Berikut disajikan Tabel 2 yang menunjukkan hasil perbandingan antara dua simulasi yang dilakukan pada kamera dan *access point*.

DOI: https://doi.org/10.33020/saintekom.v15i2.967

Tabel 2. Perbandingan Hasil Simulasi I dan Simulasi II

	Simulasi I	Simulasi II
Durasi Simulasi	3 menit	1 menit 3 detik
Gangguan Awal	00:34:08.794 - 00:35:03	23:21:06.378 - 23:21:56
Durasi Gangguan Awal	54,206 detik	49,622 detik
Pemulihan Awal	00:35:04.622 - 00:37:07	-
Durasi Pemulihan Awal	2,039 menit	-
Kamera Terputus	-	23:21:56.185 - 23:22:03.706
Durasi Kamera Terputus	-	7 detik
Gangguan Kembali	00:37:07.242 - 00:37:33	23:22:03.706 – 23:22:15
Durasi Gangguan Kembali	25,758 detik	11,294 detik
Total Durasi Gangguan	1,333 menit	1,132 menit
Kondisi Normal	00:35:04.622 - 00:37:07	-
Akhir Simulasi	00:37:33	23:22:03

Berdasarkan Tabel 2, simulasi serangan pertama berlangsung selama 3 menit. Koneksi kamera mulai terganggu pada 00:34:08 dan gangguan berlangsung sekitar 54,206 detik hingga kamera mencoba *reconnecting* yang kemudian *live viewing* kembali berfungsi pada 00:35:04.622, mempertahankan keadaan ini selama sekitar 2 menit. Kamera kembali mengalami gangguan pada 00:37:07.242 selama 25 detik hingga serangan dihentikan pada 00:37:33. Total gangguan yang terjadi dalam simulasi ini berkisar 1 menit 18 detik.

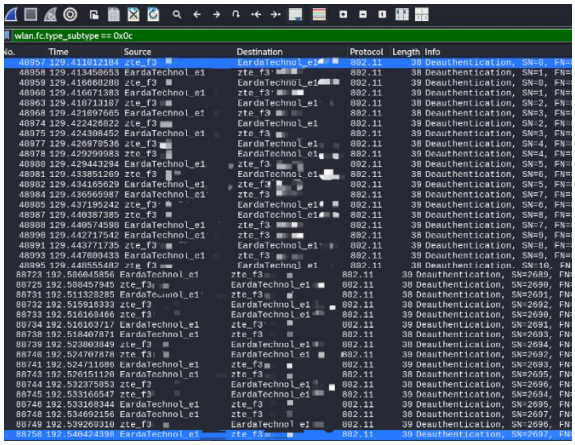


Gambar 3. *Capture packet deauthentication* Simulasi I

Sementara pada Simulasi II, serangan berlangsung selama 1 menit dan 3 detik. Koneksi kamera langsung terganggu pada 23:21:06 dan gangguan ini berlangsung selama 50 detik, menyebabkan kamera terputus dari jaringan. Kamera diarahkan untuk kembali *reconnecting* pada 23:22:03.706, dan kondisi *reconnecting* ini bertahan selama 11,294 detik hingga kembali ke fase normal pada 23:22:16.

DOI: https://doi.org/10.33020/saintekom.v15i2.967

Tidak ada fase normal atau pemulihan dalam serangan ini, sehingga total gangguan dalam simulasi ini adalah 1 menit 8 detik.



Gambar 4. *Capture packet deauthentication* Simulasi II

Berdasarkan hasil perbandingan kedua simulasi di atas, gangguan pada simulasi pertama lebih sering terjadi dengan durasi yang lebih pendek, sementara simulasi kedua mengalami gangguan yang lebih lama secara terus-menerus. Simulasi pertama memiliki fase di mana kamera kembali ke situasi normal sesaat di antara gangguan, sedangkan simulasi kedua tidak mengalami pemulihan sama sekali. Status *reconnecting* dalam simulasi kedua menunjukkan bahwa kamera masih dalam kondisi tidak berfungsi normal. Total durasi gangguan pada simulasi kedua juga jauh lebih panjang dibandingkan dengan simulasi pertama, walau dengan durasi serangan yang lebih pendek.

Beberapa strategi mitigasi yang dapat dipertimbangkan antara lain penggunaan protokol keamanan terbaru seperti WPA3, penerapan *Protected Management Frames* (PMF) untuk melindungi *frame deauthentication* dari pemalsuan, serta integrasi sistem deteksi intrusi jaringan (NIDS) yang mampu memberikan peringatan dini terhadap anomali trafik. Selain itu, pengembang kamera Wi-Fi juga dapat memperkuat mekanisme rekoneksi otomatis dan menyediakan pembaruan *firmware* secara berkala untuk menutup celah keamanan yang mungkin dieksploitasi penyerang.

4. KESIMPULAN

Simulasi serangan *deauthentication* yang diluncurkan secara *broadcast* dapat memberi pengaruh gangguan pada banyak perangkat sekaligus. Namun, efek yang ditimbulkan tidak sekuat serangan yang ditujukan langsung ke perangkat tertentu. Meskipun menyebabkan gangguan sementara pada koneksi jaringan seperti halnya pada serangan terarah, perangkat yang terdampak

DOI: https://doi.org/10.33020/saintekom.v15i2.967

dapat kembali terhubung bahkan ketika serangan masih terus berlanjut.

Serangan yang diarahkan langsung ke perangkat kamera menyebabkan perangkat terputus dari jaringan secara total. Perangkat kamera yang menjadi target pada serangan terarah tidak dapat memulihkan koneksi selama serangan terjadi, sehingga koneksi kamera dapat benar-benar terputus dan terganggu hingga akhir serangan. Hal ini dapat mengganggu fungsi pengawasan dan keamanan yang bergantung pada koneksi internet yang stabil jika terjadi pada situasi nyata.

Wireshark sangat efektif dalam mendeteksi paket *deauthentication* secara *real-time*. Alat ini memberikan informasi detail mengenai waktu, sumber, tujuan, dan *reason code* dari masing-masing paket yang menunjukkan bahwa paket dikirimkan dari pihak ketiga. Pengguna bisa dengan cepat mengidentifikasi dan menganalisis serangan yang terjadi, sehingga respon mitigasi dapat dilakukan secara cepat dan tepat.

Penelitian ini memberikan kontribusi dengan memetakan dampak serangan *deauthentication* secara langsung pada perangkat kamera berbasis Wi-Fi serta menunjukkan efektivitas Wireshark sebagai alat untuk mendeteksi paket *deauthentication* secara *real-time.* Hasil ini dapat menjadi acuan praktis bagi pengguna maupun administrator jaringan untuk menerapkan pemantauan jaringan secara aktif dan merancang strategi mitigasi yang lebih tepat sasaran. Untuk penelitian selanjutnya, pengujian dapat diperluas dengan metode deteksi berbasis otomatisasi, serta evaluasi mekanisme keamanan terbaru seperti *Protected Management Frames* (PMF) dan WPA3 untuk memperkuat perlindungan kamera Wi-Fi maupun perangkat IoT lainnya terhadap ancaman serupa.

DAFTAR PUSTAKA

Algotive. (2023). ONVIF protocol: Connecting devices for integrated video surveillance. Retrieved from https://www.algotive.ai/blog/onvif-protocol-connecting-devices-for-integrated-video-surveillance

Arora, A. (2018). Preventing wireless deauthentication attacks over 802.11 networks. arXiv preprint arXiv:1901.07301.

Aruba Networks. (2024). How IGMP process works. Retrieved from https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/multicast_6200-6300-6400-8xxx-

DOI: https://doi.org/10.33020/saintekom.v15i2.967

10000/Content/Chp_igmp/how-igm-pro-wor.htm

Arvey, S. (2022). How IGMP works. Retrieved from https://orhanergun.net/how-igmp-works

Aung, M. A. C., & Thant, K. P. (2019). IEEE 802.11 attacks and defenses.

Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.

Buchanan, C., & Ramachandran, V. (2019). Kali Linux wireless penetration testing beginner's guide (3rd ed.). Packt Publishing.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.

Flussonic. (2022). About RTSP. Retrieved from https://flussonic.com/blog/news/about-rtsp/

Gopal, S. R., Prasanth, P. R., Krishna, P. S., & Kumar, R. L. (2020). Deauthentication of IP Drones and Cameras that Operate on 802.11 WiFi Standards Using ESP8266. International Journal of Electronics and Communication Engineering and Technology, 10(2), 2019.

Gustafsson, H., & Kvist, H. (2022). Cyber Security Demonstrations using Penetration Testing on Wi-Fi Cameras.

Halton, W., & Weaver, B. (2018). Kali Linux 2018: Windows penetration testing: Conduct network testing, surveillance, and pen testing on MS Windows using Kali Linux 2018 (2nd ed.). Packt Publishing.

Hermawan, I. (2019). Metodologi penelitian pendidikan (Kualitatif, Kuantitatif, dan Mixed Method). Hidayatul Quran.

Howard. (2024). ONVIF. Retrieved from https://community.fs.com/encyclopedia/onvif.html

Korolkov, R., Kutsak, S., & Voskoboinyk, V. (2021). Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection. Bulletin of VN Karazin Kharkiv National University, series «Mathematical modeling. Information technology. Automated control systems», 50, 59-71.

Kuswanto, D. (2021). Jaringan nirkabel IEEE 802.11. Perkumpulan Rumah Cemerlang Indonesia.

Latha, R., & Bommi, R. M. (2022, December). Deauthentication attack detection in the Wi-Fi network by using ML techniques. In 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) (pp. 1-6). IEEE.

Lounis, K., Ding, S. H. H., & Zulkernine, M. (2022). Cut It:

DOI: https://doi.org/10.33020/saintekom.v15i2.967

Deauthentication attacks on protected management frames in WPA2 and WPA3. In E. Aïmeur, M. Laurent, R. Yaich, B. Dupont, & J. Garcia-Alfaro (Eds.), Foundations and Practice of Security. FPS 2021 (Vol. 13291, pp. 132–149). Springer.

Nanaware, S., Patidar, U., & Rajput, A. S. (2023). IoT security: Challenges & solutions. International Journal of Internet of Things and Web Services, 8.

Oracle Corporation. (2023). VirtualBox Overview. Diakses dari https://www.virtualbox.org/

Rakhra, T., Kaushal, A., Tanwar, S., Datta, P., & Rana, A. (2020, December). De authentication attack: A review. In 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC) (pp. 1-6). IEEE.

Research Methods in Psychology. (2023). Reliability and validity of measurement. Open Textbook Library. https://open.lib.umn.edu

Sanders, C. (2017). Practical packet analysis (3rd ed.): Using Wireshark to solve real-world network problems. No Starch Press.

Sanjaya, W. (2021). Penelitian pendidikan : jenis, metode, dan prosedur. Jakarta: Kencana.

Sanjib, S. (2018). Beginning ethical hacking with Kali Linux. Apress.

Sharma, S., & Mittal, M. (2019). Detection and prevention of de-authentication attack in real-time scenario. Int. J. Innov. Technol. Explor. Eng., 8(10), 3324-3330.

Sugiyono. (2013). Metode penelitian pendidikan: Pendekatan kuantitatif, kualitatif, dan R&D. Bandung: Alfabeta.

Sydorchuk, I. (2022). What is RTSP (Real-Time Streaming Protocol). Retrieved from https://blog.eyeson.com/what-is-rtsp-real-time-streaming-protocol

Valente, J., Koneru, K., & Cardenas, A. (2019, July). Privacy and security in Internet-connected cameras. In 2019 IEEE International Congress on Internet of Things (ICIOT) (pp. 173-180). IEEE.

Wowza Media Systems. (2024). RTSP: The Real-Time Streaming Protocol explained. Retrieved from https://www.wowza.com/blog/rtsp-the-real-time-streaming-protocol-explained

Zed, M. (2014). Metode penelitian kepustakaan. Yayasan Pustaka Obor Indonesia.

Zhuang, C. (2023). Ethical Hacking of a Smart IoT Camera: A Penetration Test on D-Link DCS 8515-LH Smart Camera

DOI: https://doi.org/10.33020/saintekom.v15i2.967