Analisis dan Pengujian *Dictionary Attack* terhadap WPA3 Berbasis *Script*

Amirah Bilqis Nuhaenibudi As-sajid[1], Ricky Eka Putra[2]

[1,2] Jurusan Teknik Informatika Fakultas Teknik Universitas Negeri Surabaya
[1]amirah.18018@mha.unesa.ac.id
[2]rickyeka@unesa.ac.id

***Abstrak*— Jaringan *Wi-Fi* sudah umum digunakan masyarakat sebagai akses internet pribadi dan umum. Jaringan *Wi-Fi* menggunakan sistem *WLAN*. Untuk membuat komunikasi *WLAN* aman, berbagai protokol standar seperti *WEP*, *WPA* dan *WPA*2 diciptakan. Meskipun demikian tidak ada satu pun di antara standar keamanan di atas yang memberikan keamanan total, dan oleh karena itu setelah 15 tahun rilisnya sistem keamanan jaringan *WPA*2, kini diluncurkannya standar baru yaitu, *WPA*3 pada tahun 2018 lalu. Sistem keamanan jaringan *WPA*3 bertujuan untuk mengamankan jaringan rumah dan perusahaan. *WPA*3 menggunakan *Dragonfly handshake* untuk menjaga keamanan jaringan sama halnya dengan *EAP-pwd* yang biasa digunakan oleh jaringan *Wi-Fi* perusahaan tertentu untuk mengautentikasi pengguna. Meskipun termasuk keamanan jaringan terkini, tetap saja ditemukannya celah pada sistem keamanan *Dragonfly handshake* milik *WPA*3 dan saat ini serangan tersebut dikenal dengan *Dragonblood attack* dimana sistem peretasannya mirip dengan *Evil-Twin attack*, namun hal itu belum bisa menjadi faktor pasti sistem keamanan terbaru ini tidak bisa diretas dengan *Dictionary attack*. Maka dari itu, penulis akan mencoba menguji celah keamanan *WPA*3 dengan serangan yang dapat meretas sistem keamanan pendahulunya, *WPA*2, untuk mengetahui seberapa aman sistem keamanan terbaru ini dibandingkan generasi sebelumnya. Uji coba peretasan ini hanya bertujuan sebagai edukasi semata, tidak diperkenankan untuk melakukan tindak kejahatan *cyber* seperti mencuri data pribadi pengguna koneksi jaringan. Dengan mengetahui sistem keamanan jaringan terbaru ini, hal ini membuktikan bahwa teknologi akan terus berkembang maju dan serangan pada celah- celah keamanan ini akan menjadi salah satu indikator evolusi perkembangan sistem keamanan yang akan datang agar menjadi lebih baik.**

Kata Kunci— ***Dictionary attack*, *WPA*2, *WPA*3, Wireshark, Shell *script*.**

I. PENDAHULUAN

Wi-Fi atau *Wireless Local Area Network* (*WLAN*) *Wi-Fi* adalah teknologi jaringan nirkabel yang menggunakan gelombang radio untuk menyediakan akses *internet* tanpa kabel dengan kecepatan yang tinggi. Adapun gelombang radio yang digunakan yakni dengan rentang 2,4 *GHz* hingga 5 *GHz*[9].

Wi-Fi juga dapat digunakan untuk menghubungkan beberapa perangkat seperti komputer *dekstop*, *laptop*, *tablet*, *smart tv*, maupun *smartphone* ke jaringan internet. Agar dapat terhubung ke jaringan *internet*, berbagai perangkat tersebut harus berada dalam satu titik akses (*hotspot*), selain untuk koneksi *internet*, *Wi-Fi* memberikan akses mudah dan *transfer* data cepat ke seluruh area jaringan kapan saja dan di mana saja[10].

Namun, penggunaan *wireless* sendiri ini pun juga menjadi salah satu celah *WLAN* yang sangat rentan terhadap serangan karena transmisi data dilakukan melalui udara. Dan melalui udara itu, menyebabkan data tersebut rentan terhadap segala jenis *cyber attack*[5].

Di awal tahun 2018, *Wi-Fi Alliance* mengumumkan bahwa *WPA*3 akan diperkenalkan dalam waktu dekat. *WPA*3 hadir dalam dua varian yaitu, *WPA*3-*Personal* dan *WPA*3-*Enterprise*, sama seperti *WPA*2[7].

Namun, meskipun sistem keamanan terus dikembangkan hingga saat ini, tidak membuat para pelaku kejahatan *cyber* untuk berhenti mencuri data pribadi pengguna jaringan. Salah satu *open source* (*OS*) seperti Kali Linux dari seri Linux yang tidak berbayar ini menjadi pilihan bagi sebagian besar *black-hat hacker* untuk meretas sistem keamanan jaringan. Tetapi, dalam kasus *WPA*3 yang memiliki peningkatan sistem keamanan enkripsi. Membuatnya jauh lebih sulit untuk diretas dibandingkan protokol keamanan sebelumnya, tetapi tidak sepenuhnya kebal terhadap serangan yang ada[2].

Kedua standar keamanan *WPA* dan *WPA*2 dikenal cukup kuat, namun keduanya dapat diretas dengan menggunakan tipe serangan *Word Reference attack*. Selain tipe serangan yang disebutkan, masih banyak tipe serangan lain yang dapat menembus celah sistem keamanan kunci enkripsi dari *modem* ataupun *router*[2].

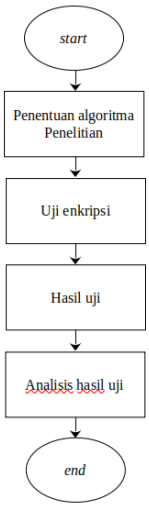
Sebagaimana dengan penjelasan di atas, maka penulis akan melakukan penelitian dengan menggunakan metode *dictionary attack* berbasis shell *script* untuk menguji ketahanan keamanan *WPA*2 dan *WPA*3, shell *script* yang digunakan menggunakan fungsi sistem *aircrack-ng* sehingga memudahkan penulis untuk mendapatkan hasil penelitian yang cepat dan akurat.

Penulis telah melakukan uji terhadap masing-masing sistem keamanan jaringan menggunakan *device* pengujian Kali linux dan perlu diperhatikan bahwasannya shell *script* yang digunakan hanya dapat diesekusi pada *device* dengan sistem operasi linux. Penelitian ini hanya digunakan untuk pembelajaran akademik saja, sehingga sangat tidak disarankan untuk melakukan pengujian diluar tujuan pembelajaran akademik.

Dengan adanya penelitian ini, diharapkan pembaca dapat mengambil langkah dengan bijak dalam menggunakan jaringan *internet* umum, dan dapat meminimalisir kemungkinan terjadinya pembobolan data jaringan pribadi.

II. METODE PENELITIAN

Penyerangan menggunakan shell *script dictionary attack*. Hasil pengujian pada sistem kemanan jaringan *portable hotspot* milik *smartphone* akan menjadi pendukung validasi kinerja sistem keamanan jaringan terbaru dibanding versi sebelumnya:



Gambar.1 Alur penelitian

Penelitian ini memiliki berbagai tahapan pada prosesnya agar mendapatkan hasil dalam suatu penelitian yang berhasil seperti diuraikan pada gambar 3.1 Adapun penjelasan tiap tahapan akan dijelaskan sebagai berikut:

A. Penentuan algoritma penelitian

Tahap pertama yaitu penentuan algoritma penelitian. Dalam penelitian akan menggunakan algoritma metode enkripsi dengan tipe serangan '*dictionary attack*'.

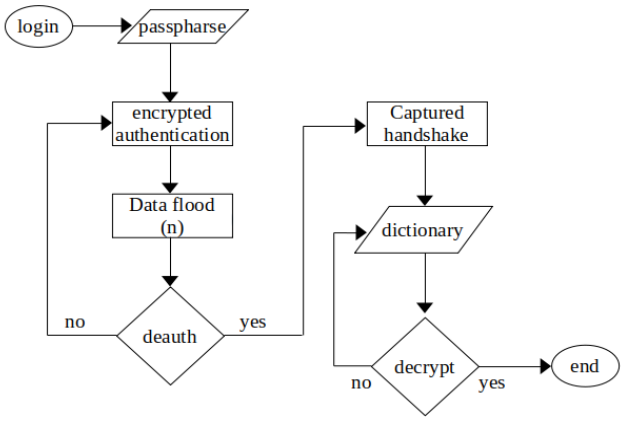
Selain itu, algoritma yang akan ditentukan adalah:

1. Jenis keamanan jaringan *Access Point* (*smartphone*)
   Jenis keamanan yang akan diuji adalah keamanan jaringan terbaru *WPA3-Personal* dan keamanan jaringan lama *WPA2-personal* sebagai pembandingnya.
2. Jenis perangkat yang akan menjalankan *dictionary attack*
   Perangkat yang digunakan adalah *laptop* HP ProBook 4440s berbasis *OS* kali linux untuk mempermudah dan mempercepat proses *cracking*.
3. Metode *dictionary attack*
   Yang terakhir adalah metode yang digunakan dalam uji enkripsi adalah shell *script aircrack-ng*.

B. Uji enkripsi

Uji enkripsi yang akan dilakukan menggunakan metode *dictionary attack* berbasis shell *script aircrack-ng*, uji ini akan menyerang transmisi enkripsi pada masing-masing keamanan jaringan pada kondisi *online*. Transmisi yang berhasil terekam akan didekripsikan untuk mengetahui celah keamanan jaringan sebagai tolak ukur perbandingan keamanan jaringan yang akan diuji.

Perangkat yang akan menjadi *access point* akan diubah sistem keamanan jaringannya bergantian secara runtut setelah satu jenis keamanan selesai diuji dengan tahapan yang sama agar dapat diketahui pada titik pengujian mana terjadinya perbedaan hasil sehingga dapat ditarik sebagai data hasil saat dilakukan analisis hasil uji.



Gambar.2 *Flowchart* uji enkripsi

C. Hasil uji

Informasi *password* yang telah didekripsi akan diuji kebenaran dan keakuratan dengan uji *login* pada perangkat jaringan lainnya yang belum pernah terhubung dengan jaringan yang diretas pada penelitian saat ini, apakah perangkat asing dapat berhasil terhubung dengan *password* yang berhasil diretas atau tidak.

D. Analisis hasil uji

Data hasil uji akan dianalisis lebih detail demi mendapatkan pembuktian akan adanya perbedaan dari kedua sistem keamanan jaringan yang telah diuji sehingga dapat ditarik kesimpulan dan memenuhi tujuan penelitian.

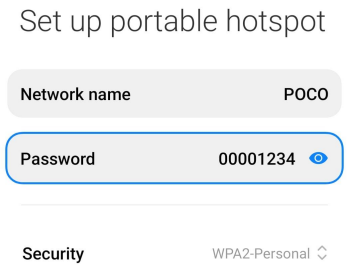
III. HASIL DAN PEMBAHASAN

Metode yang akan digunakan dalam pengambilan data analisis, yaitu, based *dictionary attack* menggunakan *tools aircrack-ng*. *Tools* ini sangat populer digunakan oleh kalangan *hacker* pemula, kelebihan *tools* ini mudah digunakan, namun kekurangan *tools* ini hanya bisa digunakan untuk *based dictionary attack* tanpa ada kombinasi.

A. Uji enkripsi *aircrack-ng*

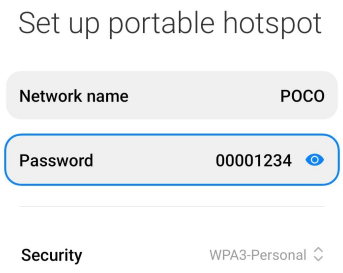
1. Uji shell *script*

Langkah pertama yang perlu dilakukan adalah mengatur *setup access point*. Pada uji saat ini akan dilakukan pada 2 keamanan jaringan yang berbeda, *WPA2-Personal* dan *WPA3-Personal*.



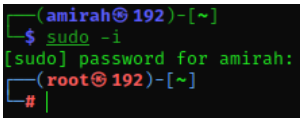
Gambar.3 *Setup WPA2-Personal*

Gambar.4 *Setup WPA3-Personal*



Langkah berikutnya persiapkan perangkat yang menjadi penyerangnya. Mode monitor yang diaktifkan akan menyebabkan perangkat tidak bisa terhubung ke internet saat mulai berlangsungnya penyerangan, karena *wireless adapter* akan merubah haluan dari menghubungkan jaringan menjadi mengawasi dan menangkap *traffic packet data* pada seluruh jaringan yang tersedia secara *live*.

Untuk memulai mode monitor, hal pertama yang harus dilakukan adalah buka *terminal* kali linux dan masuk ke mode *root*:



Gambar.5 fungsi *root* pada kali linux

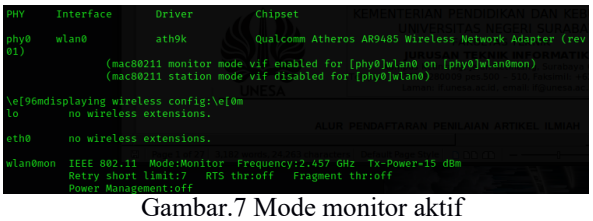
Berikutnya, aktifkan mode monitor jaringan dengan menggunakan shell *script* airmon-ng:

```
#!/usr/bin/sh
#amirah@18

echo "\e[92mstarting airmon on device 'wlan0'\e[0m"
airmon-ng start wlan0
sleep 5

echo "\e[96mdisplaying wireless config:\e[0m"
iwconfig
sleep 5
```

Gambar.6 Shell *script* Airmon-ng

Untuk memasukan shell *script* pada *terminal*, gunakan fungsi *sudo bash* dilanjutkan dengan direktori file shell *script*.

Setelah *script* dijalankan, mode monitor jaringan akan aktif dan perangkat sementara waktu tidak dapat terhubung dengan jaringan *internet.* Berikut tampilan mode monitor saat berhasil diaktifkan:



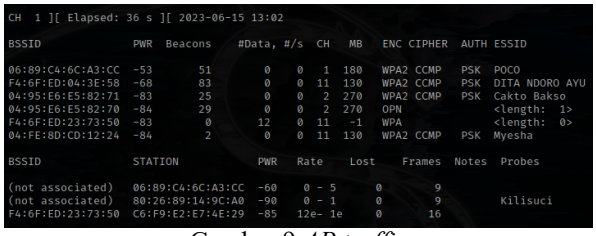
Gambar.7 Mode monitor aktif

Lalu, setelah mode monitor berhasil diaktifkan, langkah berikutnya adalah menangkap *AP traffic* yang aktif di sekitar perangkat menggunakan shell *script* Airodump-ng:

```
#!/usr/bin/sh
#amirah@18
echo "\e[96mcapturing packets from monitor device:\e[0m"

airodump-ng wlan0mon
sleep 5
```

Gambar.8 Shell *script* Airodump-ng

Jika shell *script* telah dieksekusi dengan benar, maka akan muncul tampilan seperti ini:



Gambar.9 *AP traffic*

Berikutnya fokuskan *AP traffic* pada bssid *AP* yang akan diuji dengan menggunakan shell *script* lanjutan:

```
#!/usr/bin/sh
#amirah@18
#bssid target
echo "\e[96mcapturing packets from monitor device:\e[0m"

airodump-ng -c 1 -bssid () wlan0mon
sleep 5
```

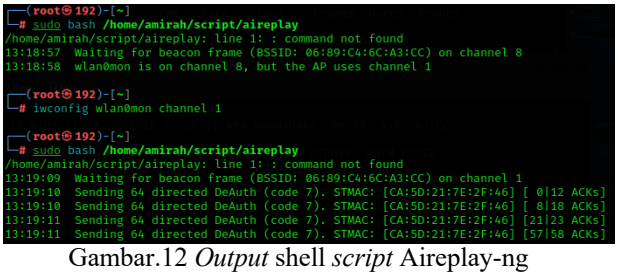
Gambar.10 *Output* fokus *AP traffic*

Langkah berikutnya merupakan langkah yang krusial dalam uji coba ini, yaitu menangkap *packet handshake* pada jaringan yang aktif (*online*). Pertama, cara yang akan digunakan adalah *deauthentication* perangkat yang terhubung dengan *AP* target uji. Berikut shell *script* Aireplay-ng yang akan digunakan:

```
#!/bin/bash
#amirah@18
#A="x" AP
#C="x" STATION
#0= (x)times

sudo aireplay-ng -0 () -a () -c () wlan0mon
sleep 5
```

Gambar.11 Shell *script* Aireplay-ng

Tampilan *output shell script* Aireplay-ng:



Gambar.12 *Output* shell *script* Aireplay-ng

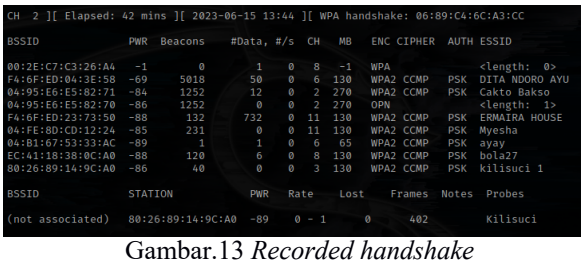
Dapat dilihat pada gambar, bahwa eksekusi shell *script* Aireplay-ng sempat tertunda sekali dikarenakan jaringan monitor perangkat tidak berada di *channel* yang sama dengan *AP* target, hal ini wajar terjadi karena *wireless adapter* perangkat aktif berpindah *channel* karena sedang dalam mode monitor ke seluruh *AP* yang berada pada jangkuan perangkat.

Untuk mempercepat fokus monitor tertuju pada channel target, dapat menggunakan fungsi:

```
iwconfig wlan0mon channel 1
```
atau
```
airodump-ng wlan0mon 1
```

Channel dapat diubah sesuai dengan fokus kebutuhan pengguna.

Jika perangkat *receiver* jaringan target berhasil terputus sementara dengan *AP* target dan menghubungkan kembali di saat *AP traffic* aktif menangkap transmisi *packet data*, maka akan terekam *handshake* dari transmisi kode yang telah berlangsung, tampilan *output shell script* Airodump-ng sebelumnya akan berubah menjadi seperti berikut:

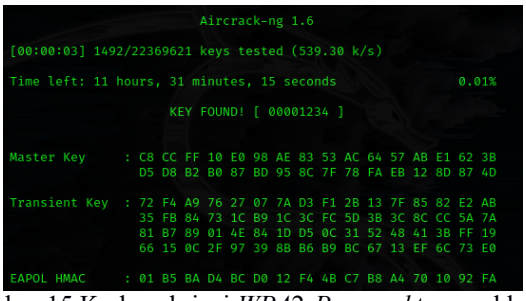


Gambar.13 *Recorded handshake*

Langkah terakhir adalah dekripsi kode enkripsi yang telah didapat menggunakan shell *script* Aircrack-ng, berikut adalah shell *script* Aircrack-ng:

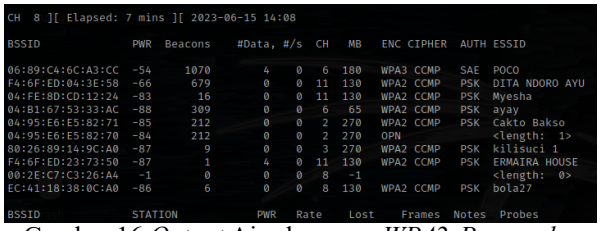
```
#!/bin/bash
#amirah@18
#B=captured handshake
#W=dictionary address
echo "\e[96mcapturing packets from monitor device:\e[0m"
capfile="$(find /root/Downloads/captures/ -type f -name '*.cap')"

aircrack-ng ().cap -b () -w ()
sleep 5
```
Gambar.14 *Shell script* Aircrack-ng

Setelah melalui proses dekripsi kode, akan didapatkan sandi keamanan untuk mengakses *AP* target seperti gambar di bawah ini:

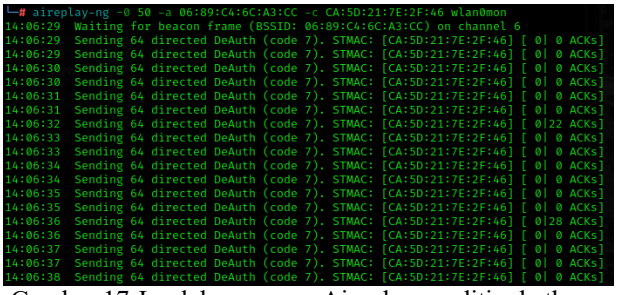


Gambar.15 Kode enkripsi *WPA2-Personal* terpecahkan

Namun *output* pada keamanan jaringan *WPA3-Personal* tidak sama dengan gambar di atas, melainkan:



Gambar.16 *Output* Airodump-ng *WPA3-Personal*



Gambar.17 Jumlah serangan Aireplay-ng ditingkatkan

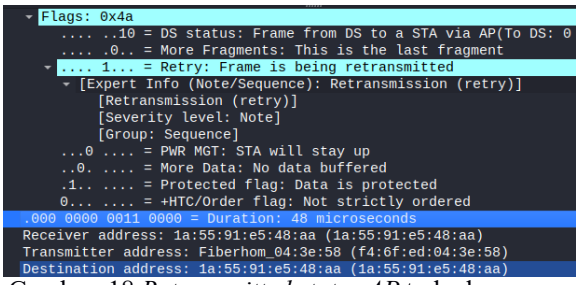
Dapat dilihat bahwa meskipun jumlah serangan shell *script* aireplay-ng ditingkatkan dari 20 putaran hingga 50 putaran, tetap tidak terjadi kebocoran rekaman transmisi antara perangkat jaringan yang terhubung dengan *AP* target dan *AP* target itu sendiri. Perangkat jaringan juga tidak terdampak dari banyaknya serangan yang dilakukan Aireplay-ng, berbeda dengan keamanan *WPA2-Personal* yang hubungan jaringannya langsung terputus meskipun jumlah serangan belum lengkap atau kurang dari 20 putaran.

Alhasil, eksekusi shell *script* Aircrack-ng tidak dibutuhkan pada tahap uji enkripsi langsung dengan *AP* target *WPA3-Personal*, dan berhenti sampai tahap shell *script* Aireplay-ng.

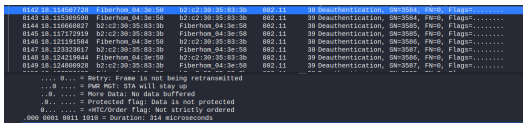
2. Uji wireshark

Berikut hasil rekaman waktu transmisi data saat diluncurkannya serangan *script* aireplay-ng demi mendapatkan *capture handshake* menggunakan *packet capture* wireshark.

a. Data transmisi WPA2

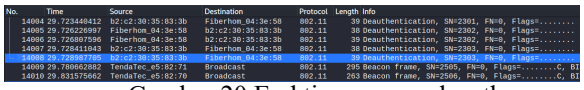


Gambar .18 *Retransmitted status AP* terhadap *user*



Gambar.19 *Start time* proses *deauth*

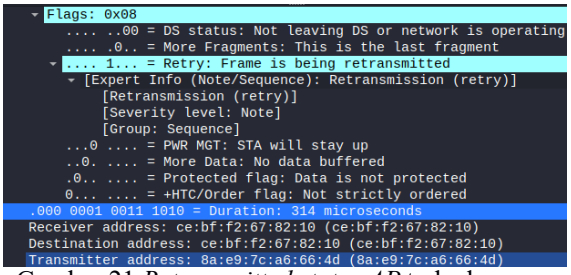
Terlihat bahwa pada saat autentikasi ulang, *script* menyerang dengan mengirimkan traffic transmisi data dalam jumlah besar sehingga menyebabkan gangguan dan hal ini menyebabkan terputusnya hubungan antara *user* dengan *AP*, dikarenakan pada sistem keamanan *WPA*2 yang masihmenggunakan 802.11 *OA*. Teknik penyerangannya dengan eksploitasi kontrol frame pada 802.11 *OA* dengan mengirim *data packet* palsu sebagai *user* lain yang tidak terautentikasi kepada titik *AP*, dan *data packet* palsu sebagai *AP* lain yang mengindikasi bahwasannya user perlu melakukan autentikasi ulang kepada titik *user*.



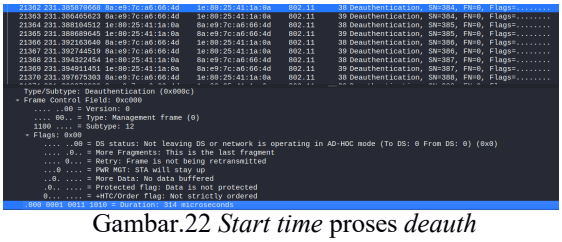
Gambar.20 End time proses deauth

Setelah berhasil membanjiri sistem autentikasi dengan *data packet* palsu, *user* yang tidak menggunakan *PMK* akan memasukan kembali kata sandi pada perangkat mereka, sehingga akan muncul rekaman packet "*WPA Handshake*=" karena memulai kembali autentikasi dari awal, sedangkan apabila informasi *login* telah disimpan menggunakan *PMK*, maka akan muncul rekaman *packet* "*PMKID*=", *key caching*-lah yang tertangkap, karena antara *user* dan *AP* tidak terjadi autentikasi ulang.

b. Data transmisi *WPA2*

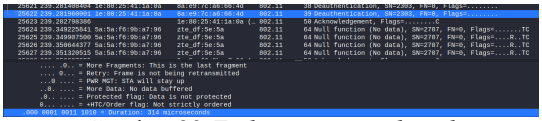


Gambar.21 *Retransmitted status AP* terhadap *user*



Gambar.22 *Start time* proses *deauth*

Proses serangan deautentikasi terhadap *WPA*3 tetap terbaca pada *packet tracer* wireshark, sama halnya dengan sistem keamanan sebelumnya.



Gambar.23 *End time* proses *deauth*

Waktu yang diperlukan tidak jauh berbeda, namun hasil yang dicapai juga berbeda, hal ini membuktikan peningkatan keamanan dari *WPA*3 dari pendahulunya *WPA*2.

B. Analisis hasil uji

Berdasarkan hasil uji enkripsi bahwasannya terlihat adanya perbedaan sistem keamanan, beberapa variabel yang bisa menjadi perbandingan dari kedua sistem keamanan yang diujikan mendapatkan perlakuan yang sama, oleh karena itu, didapatkan beberapa hasil data berikut berdasarkan pengujian di atas:

1. Tabel hasil variabel pengujian

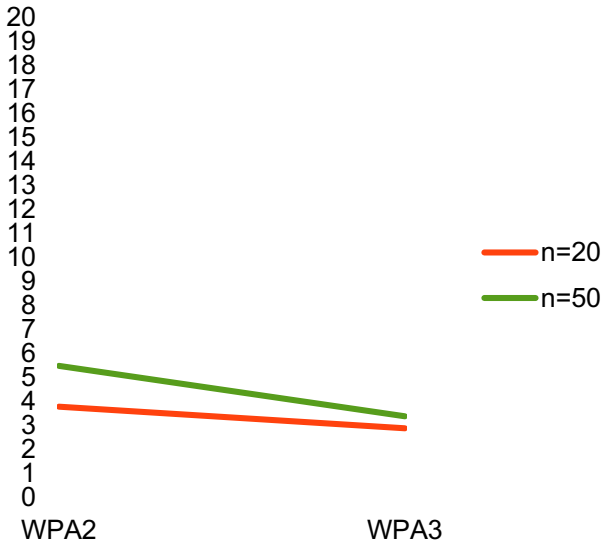
No.	Tahap serangan	Var uji	Status	
			WPA2	*WPA3*
1.	*Capture traffic AP*	*MAC Address Beacon Cipher Auth system*	Berhasil	Berhasil
2.	*Dauthentic ation*	*MAC Address Beacon*	Berhasil	Tidak Berhasil
3.	*Captured handshake*	*Auth system*	Berhasil	Tidak Berhasil
4.	*Dictionary decryption*	*Cipher*	Berhasil	Tidak Berhasil

Deauthentication MAC Address AP terhadap *user* berhasil dilakukan pada sistem keamanan *WPA*2, sedangkan pada *WPA*3 sebaliknya. Sehingga untuk tahap *captured handshake* hingga *dictionary decryption* tidak mungkin dilakukan pada *WPA*3.

2. Tabel waktu *capture handshake*

No.	*WPA2*		*WPA3*		Putaran (n)	Status	
	Start (s)	*End (s)*	*Start (s)*	*End (s)*		*WPA2*	*WPA3*
1.	18.1	21.9	231.9	234.8	20	Berhasil	Tidak Berhasil
2.	24.2	29.7	235.8	239.2	50	Berhasil	Tidak Berhasil

Meskipun putaran serangan *deauthentication* diperkuat menjadi 50x, proses deauthentication tetap tidak berhasil terhadap *WPA*3.



Grafik.1 Perbandingan waktu (s) terhadap putaran deauth (n)

Pada grafik di atas terlihat bahwa meski jumlah putaran serangan *deauthentication* bertambah pada *WPA*3 namun, waktu yang diperlukan untuk proses deauthentication lebih sedikit dibanding *WPA*2. Hal ini yang menjadi pembuktian adanya peningkatan keamanan *dragonfly handshake* milik diffie-hellman yang terproteksi oleh *SAE* dimana telah didukung sistem autentikasi enkripsi oleh *OWE* untuk mencegah *captured key caching* yang diamankan kembali oleh *temporal secret key* milik *PFS*.

IV. KESIMPULAN

Dari penggabungan hasil uji dan hasil analisis, dapat ditarik kesimpulan bahwasannya *WPA*3-*Personal* dapat menangkal *dictionary attack* dikarenakan pertambahan sistem keamanan *key exchange protocol Dragonfly handshake* atau bisa disebut juga Diffie-Hellman *key protocol* yang dimiliki *WPA*3-*Personal* telah didukung *Perfect forward secrecy* serta *OWE* yang dimana sistem ini dapat mencegah teretasnya rekaman transmisi kode saat *user* terhubung dengan *AP* yang telah dibekali sistem keamanan *WPA*3-*Personal*.

Namun sayangnya, *WPA*3-*Enterprise* tidak didukung sistem *key exchange protocol* terbaru ini dikarenakan jumlah pengguna yang sangat banyak. Meskipun demikian, hal ini telah diantisipasi dengan menggunakan autentikasi terbaru *OWE* yang dapat meminimalisir adanya serangan *crack* seperti *dictionary attack* meskipun tanpa ada *key exchange protocol* dalam transmisi datanya. Tetapi, tidak bisa dikatakan bahwa sistem keamanan terbaru ini sepennuhnya akan aman dari serangan kejahatan *cyber*. seperti pendahulunya, *WPA*2 yang menggunakan sistem keamanan *Pre-Shared Key* dan 4-*way handshake* pada awal diterbitkannya, para penjahat *cyber* atau biasa dikenal *black hat hacker* akan terus mencari celah keamanan.

V. SARAN

Berdasarkan hasil dan kesimpulan penelitian ini, peneliti memberikan beberapa saran untuk kepentingan penelitian selanjutnya:

Pertama, disarankan untuk melakukan pengujian sistem keamanan *WPA*3 yang lebih variatif seperti kombinasi metode tipe serangan *dictionary* dengan lainnya.

Kedua, dilakukannya pengujian kerentanan keamanan sistem *WPA*3-*Enterprise*.

Ketiga, melakukan penelitian mengenai pencegahan serangan tipe *phising* basis sistem sehingga memudahkan *user* untuk tetap otomatis mencoba terhubung dengan halaman *login AP* asli tanpa perlu memilih *AP* secara manual pada perangkat *user* yang menyebabkan potensi terjebak pada *AP phising*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih banyak serta rasa syukur kepada Allah SWT Yang Maha Pengasih lagi Maha Penyayang atas dimudahkannya dalam menulis penelitian ini, sehingga dapat terselesaikan dengan baik. Tidak lupa juga sholawat serta salam kepada Nabi Muhammad SAW. Kemudian saya ucapkan banyak terima kasih kepada keluarga saya terutama untuk nenek saya yang tercinta senantiasa mendukung dan mendoakan saya. Dan saya ucapkan terima kasih banyak kepada dosen pembimbing saya, bapak Dr. Ricky eka, S.Kom, M.Kom., yang telah membimbing saya dengan sabar hingga penulisan penelitian ini rampung dengan baik, serta para penguji yang telah memberikan banyak masukan terhadap penulisan penelitian ini. Terakhir, rasa terima kasih saya berikan kepada teman-teman jurusan yang saya cintai karena telah mendukung dan mendorong saya untuk tidak menyerah dalam menyelesaikan penelitian ini.

REFERENSI

Alliance, W.-F. (2018). *WPA3 Specification Version 1.0*. Retrieved from Wi-Fi: https:/www.wi-fi.org/file/wpa3-specification-v10

Ardiyansyah S, V., & Raharjo, S. (2021). Pengaruh Wireless Security Protocol pada Throughput Jaringan Wireless 802.11ax. *Paradigma*, 5-6.

Beal, V. (2021). *Definitions Wi-Fi*. Retrieved from Webopedia: https://www.webopedia.com/definitions/wifi/

Bhatia, P., & Sumbaly, R. (2014). Framework for Wireless Network Security Using Quantum Cryptography. *IJCNC*, 5-7.

Buczkowski, M. (2018). *Wi-Fi Security Evolution*. Retrieved Juni 15, 2023, from Grand Metric: https:/www.grandmetric.com

Calibus, C. (2018, Juni 15). *Attacks Against Wi-Fi Networks are Listed and Whether or Not WPA3 Addresses These*. Retrieved from Research Gate: https://www.researchgate.net/figure/Attacks-against-Wi-Fi networks-are-list-and-whether-or-not-WPA3-addreses-these_tbl1_328632250

Freudenrich, J., Weidman, J., & Grossklags, J. (2022). Responding to KRACK: Wi-Fi Security Awareness in Private Households. *HAL Open Science*, 2-5.

Harkins , D. (2017). Opportunistic Wireless Encryption. *IETF RFC 8110*, 4-10.

Harkins, D. (2012). Secure Pre-Shared Key (PSK) Authenticaton for the Internet Key Exchance Protocol (IKE). *IETF RFC 6617*, 5-11.

Harkins, D. (2015). Dragonfly Key Exchange . *IETF RFC 7664*, 4-13.

Indonesia, C. (2022). *Wi-Fi: Pengertian, Fungsi, dan Cara Kerja*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20220222 14121-190-765473/wifi-pengertian-fungsi-dan-cara-kerja

Jena, B. K. (2023). *What is AES Encryption and How Does it Works*. Retrieved June 26, 2023, from Simplilearn: https:/www.simplilearn.com

Kumar O., D. N. (2021). WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircracking Technique. *ICCMC*.

Network, A. (2023). *Perfect Forward Secrecy (PFS)*. Retrieved juli 26, 2023, from avinetwork: https:/www.avinetworks.com

Ramadhan, A. (2017, Juni 15). *Ancaman Keamanan Jaringan Wireless Rumahan*. Retrieved from https://www.belajarsys.net/keamanan-jaringan-wireless-rumahan-evil-twin-attack

Shadeed, I., & Rasheed A, D. (2020). Analyzing and Evaluating the Security Standards in Wireless Network. *A Review Study: IJCI* , 5-7.

Singh, R., & Sharma, T. (2019). An Overview of WLAN Security. *ISJTR*, 1-2.

Srikanth , V., & Reddy, D. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2, & WPA3) . *IJSRCSEIT*, 3-6.

V. Srikanth, D. I. (2019). Wireless Security Protocols: JETIR Research Journal. *JETIR Research Journal*.

Vanhoef, M., & Ronen , E. (2019). A Security Analysis of WPA3's SAE Handshake. *Cryptology ePrint Archive*, 2-10.

Vanhoef, M., & Ronen, E. (2019). Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *Cryptology ePrint Archive*, 3-6.

Ward, L. (2023). *WPA2 vs WPA3*. Retrieved Juli 26, 2023, from Natapa: https:/id.natapa.org