ANALISIS PERBANDINGAN KINERJA DAN KEAMANAN PROTOKOL *WPA2* DAN *WPA3* DENGAN METODE *PENETRATION TESTING*

Yudi Mulyanto[1], Shindyka Syalu Qanita[2], Dimas Wiryatari[3], Farida Idifitriani[4]

[1234]Program Studi Informatika, Universitas Teknologi Sumbawa

Jl. Raya Olat Maras, Batu Alang, Moyo Hulu, Sumbawa, NTB 84371
[1] yudi.mulyanto@uts.ac.id, [2] shindykasyalu@gmail.com, [3] dimas.wiryatari@uts.ac.id,
[4]farida.idifitriani@uts.ac.id

Abstract

Sumbawa University of Technology is one of the universities whose network utilizes the WPA2 security protocol, but during its use, the WPA2 security protocol has hacked the network. This study aims to analyze the performance comparison of the WPA2 and WPA3 security protocols at the Faculty of Systems Engineering, Sumbawa University of Technology by identifying the weaknesses and advantages of each protocol. In this study the authors used a mixed methods research method, namely a combination of qualitative research and quantitative research. Qualitative research in this study involves collecting data through observation and literature study and using experimental methods to compare the WPA2 and WPA3 protocols. And the analysis method used is Penetration Testing by simulating attacks on the two security protocols. The attack carried out is a dictionary attack using tools on the Kali Linux operating system. The results show that WPA3 shows better resistance to most attacks, especially handshake and protection against password cracking, thus making WPA3 a more secure choice for wireless networks. This is because WPA3 uses Simultaneous Authentication of Equals (SAE) authentication which has the advantage of using the Password-Authenticated Key Exchange (PAKE) algorithm that can protect passwords from unauthorized third parties.

Keywords : *analysis, WPA2, WPA3, penetration testing, wireless security*

Abstrak

Universitas Teknologi Sumbawa merupakan salah satu universitas yang jaringannya memanfaatkan protokol keamanan WPA2, namun selama penggunaannya protokol keamanan WPA2 pernah terjadinya peretasan pada jaringan tersebut. Penelitian ini bertujuan untuk menganalisis perbandingan kinerja protokol keamamanan WPA2 dan WPA3 di Fakultas Rekayasa Sistem Universitas Teknologi Sumbawa dengan mengidentifikasi kelemahan dan kelebihan dari masing – masing protokol. Pada penelitian ini penulis menggunakan metode penelitian metode campuran *(mixed methods)* yaitu kombinasi penelitian kualitatif dan penelitian kuantitatif. Penelitian kualitatif pada penelitian ini melibatkan pengumpulan data melalui observasi dan studi pustaka dan menggunakan metode eksperimen untuk membandingkan protokol WPA2 dan WPA3. Serta metode analisis yang digunakan ialah *Penetration Testing* dengan melakukan simulasi serangan terhadap kedua protokol keamanan tersebut. Serangan yang dilakukan ialah *dictionary attack* menggunakan *tools-tools* pada sistem operasi Kali Linux. Dari hasil penelitian menunjukkan bahwa WPA3 menunjukkan ketahanan lebih baik terhadap sebagian besar serangan, terutama *handshake* dan perlindungan terhadap *cracking password*, sehingga menjadikan WPA3 pilihan yang lebih aman untuk jaringan nirkabel. Hal ini dikarenakan WPA3 menggunakan autentikasi *Simultaneous Authentication of Equals* (SAE) yang memiliki kelebihan menggunakan algoritma *Password-Authenticated Key Exchange* (PAKE) yang dapat melindungi kata sandi dari pihak ketiga yang tidak berwewenang.

Kata kunci : *analisis, WPA2, WPA3, penetration testing, wireless security*

1. PENDAHULUAN

Keamanan jaringan komputer merupakan komponen penting dari sistem apa pun. Sistem keamanan jaringan komputer perlu dilindungi dari intrusi dan upaya pihak yang tidak berwenang untuk memindai atau menyusup [1]. Seiring dengan meningkatnya pengguna internet dan perangkat yang terhubung, potensi serangan *cyber* juga semakin meningkat. Dalam hal ini, protokol keamanan WPA2 dan WPA3 menjadi sangat berkaitan untuk dianalisis, mengingat keduanya dirancang untuk melindungi data yang dikirim melalui jaringan nirkabel.

Wi-Fi Protected Access 2 adalah metode yang disetujui *WIFI Alliance* untuk perlindungan data. WPA2 dibangun menggunakan algoritma AES dan CCMP [2]. Meskipun menawarkan tingkat keamanan yang lebih baik dibandingkan pendahulunya, WPA2 masih memiliki beberapa kelemahan yang dapat disalahgunakan oleh peretas. Di sisi lain, WPA3 yang diluncurkan pada tahun 2018, menawarkan keamanan yang lebih kuat dan fitur keamanan yang lebih baik, seperti enkripsi individual dan perlindungan terhadap serangan *Brute-Force* [3]. WPA3 merupakan evolusi dari protokol keamanan. WPA3 dirancang untuk memberikan tingkat keamanan yang lebih tinggi dibandingkan protokol WPA2 [4].

Universitas Teknologi Sumbawa merupakan salah satu universitas swasta yang berada di Kabupaten Sumbawa, Nusa Tenggara Barat. Universitas ini khususnya Fakultas Rekayasa Sistem yang masih memanfaatkan protokol keamanan WPA2 untuk keamanan jaringan nirkabelnya, meskipun protokol keamanan terbaru yaitu WPA3 telah tersedia. Selama penggunaan protokol WPA2 pernah terjadinya kebobolan atau peretasan pada jaringan tersebut. Oleh karena itu penulis melakukan perbandingan kinerja kedua protokol tersebut.

Penetration Testing adalah metode yang efektif digunakan untuk mengevaluasi keamanan jaringan dengan melakukan proses simulasi serangan untuk mengidentifikasi celah keamanan dalam system [5]. Pentesting juga dikenal sebagai pengujian penetrasi, menyimulasikan serangan aktual untuk mengevaluasi bahaya dari kemungkinan celah keamanan [6]. Dengan menggunakan metode ini, penulis dapat menilai seberapa baik protokol WPA2 dan WPA3 dapat bertahan terhadap berbagai teknik serangan *dictionary attack*. Proses *penetration testing* menggunakan sitem operasi Kali Linux yang sudah diinstal pada VM *VirtualBox* dan menggunakan *tools-tools* Kali Linux seperti *airmon-ng, airodump-ng, aireplay-ng,* dan *aircrak-ng. VirtualBox* merupakan software yang memungkinkan menjalankan sistem operasi lain sebagai *Guest* OS dalam lingkungan virtual seperti Kali Linux [7]. Kali Linux adalah penerus platform pengujian penetrasi *BackTrack* yang secara umum dianggap sebagai paket alat standar [8].

Perbandingan kinerja protokol WPA2 dan WPA3 melalui *penetration testing* tidak hanya bertujuan untuk mengidentifikasi kelemahan dari masing-masing protokol tetapi juga memberikan rekomendasi untuk meningkatkan keamanan jaringan nirkabel secara keseluruhan. Dengan memahami perbedaan dalam ketahanan kedua protokol ini terhadap serangan *cyber,* organisasi dapat mengambil langkah-langkah yang efektif untuk melindungi data sensitif mereka. Selain melalui *penetration testing,* penulis juga mengukur parameter *Quality of Service* (QoS) untuk menilai kinerja protokol keamanan WPA2 dan WPA3 di beberapa perangkat *smartphone*. *Quality of Service* adalah istilah jaringan yang menggambarkan tingkat keandalan dan kecepatan pengiriman berbagai jenis data selama komunikas [9]. *QoS* didefinisikan sebagai kemampuan suatu jaringan untuk menawarkan layanan yang lebih baik untuk lalu lintas jaringan tertentu menggunakan berbagai teknologi dan upaya untuk mengkarakterisasi sifat dan atribut suatu layanan [10].

Beberapa penelitian yang memiliki keterkaitan dengan penelitian yang penulis lakukan. Penelitian yang dilakukan oleh [11] menggunakan metode *Penetration Testing* untuk membandingkan sistem keamanan WPA2-PSK dan *Captive Portal* bahwa WPA2-PSK memiliki sistem keamanan yang lebih baik dari pada *captive portal,* Di mana dari 10 sampel yang diujikan hanya 2 sampel yang berhasil didapatkan *password* WPA2-PSK dan berhasil masuk ke jaringan. Penelitian selanjutnya dilakukan oleh [12] penelitian ini mendapatkan kerentanan pada serangan *Dictionary Attack, Evil Twin, Traffic Control, dan Handsake Capure.* Dari pengujian tersebut membuktikan bahwa keamanan jaringan yang menggunakan protokol WPA3 masih memiliki kerentan terhadap celah untuk dieksploitasi. Penelitian [13] bahwa hasil uji coba dan analisis yang dilakukan pada penelitian ini di

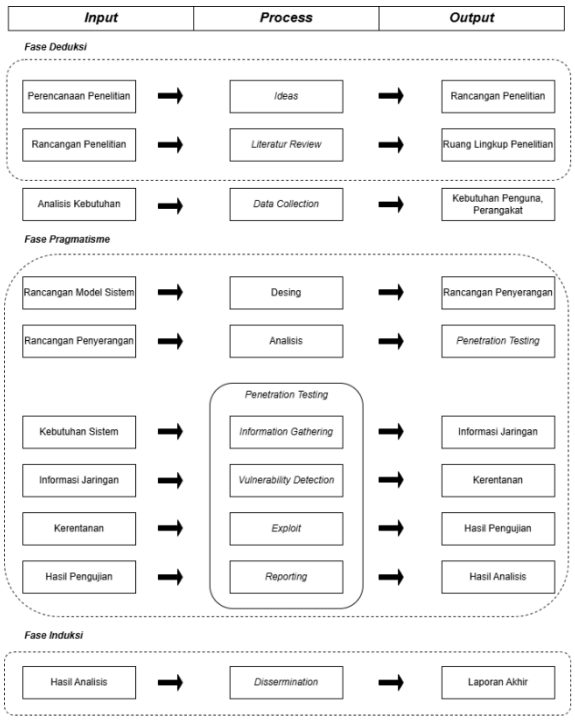
dapatkan bahwa WPA3 dapat menangkal *Dictionary Attack* dikarenakan adanya penambahan sistem keamanan yaitu *Diffie-Helman key protocol*, dimana sistem keamanan ini dapat mecegah teretasnya rekaman transmisi kode yang sudah terhubung dengan AP yang memiliki sistem keamanan WPA3. Hasil dari Penelitian [4] dilakukan uji coba 3 *type* serangan yaitu *Cracking The Encryption, Bypassing MAC address Authantication*, dan *Attacking The Infrastructure*. Dari tiga serangan hanya satu serangan yang memiliki status gagal, yaitu *Bypassing MAC Address Authenticcation.* Hali ini membuktikan bahwa pada TP-Link Archer A6 masih banyak memiliki kelemahan oleh karena itu masih diperlukan peningkatan keamanan pada TP-Link Archer A6. Penelitian lainnya [5] hasil pengujian yang dilakukan dapat diketahui bahwa, metode *Mac Changer* sistem keamanan WPA2 pengguna tidak berhak dapat mengetahui alamat MAC jaringan *wireless* karena belum masuk pada jaringan *wireless* yang dituju, dan menggunakan metode *signal scanning* penyedia jaringan *wireless* dapat mendeteksi IP yang mencurigakan pada sistem keamanan WPA2.

Berdasarkan permasalahan yang telah diidentifikasikan dan berbagai penelitian yang diuraikan, maka penulis melakukan penelitian terkait perbandingan kinerja antara protokol keamanan WPA2 dan WPA3 guna mengetahui kelemahan dan kelebihan dari kedua protokol tersebut. Penelitian yang penulis lakukan menggunakan metode *Penetration Testing* dengan melakukan penyerangan dengan *dictionary attack* untuk kedua protokol keamanan dan melakukan pengukuran terhadap parameter *Quality of Service (QoS)* untuk melihat kinerja kedua protokol tersebut dengan beberapa perangkat yang mendukung baik protokol keamanan WPA 2 maupun WPA 3.

2. METODOLOGI PENELITIAN

2.1. Skema Alur Penelitian

Kombinasi pendekatan penelitian kualitatif dan kuantitatif, yang dikenal sebagai metode campuran [14], digunakan dalam penelitian ini. Karena sifat masalah yang mencirikan keadaan subjek atau objek yang diteliti secara deskriptif dengan kecenderungan analisis, penelitian kualitatif dalam penelitian ini melibatkan pengumpulan data melalui observasi dan telaah Pustaka [15]. Dalam penelitian kuantitatif menghasilkan banyak temuan yang dapat diperoleh dengan menggunakan beberapa prosedur statistik atau metode kuantitaf pengukuran [16]. Pada penelitian ini, penelitian kuantitatif dilakukan untuk membandingkan protokol WPA2 dan WPA3 dengan mengukur parameter QoS. Meskipun pengujian QoS dan evaluasi keamanan memiliki focus yang berbeda tetapi keduanya memiliki keterkaitan. Parameter QoS yang buruk dapat menunjukkan adanya serangan atau aktivitas mencurigakan yang dapat mempengaruhi kinerja jarinngan. Dan melakukan eksperimen untuk melakukan uji coba serangan terhadap kedua protokol keamanan WPA2 dan WPA3. Metode Eksperime melaksanakan penyelidikan yang objektif, metodis, dan terkendali untuk memprediksi suatu fenomena [17]. Pendekatan *Penetration Testing* digunakan dalam rencana analisis. Diagram alur penelitian ditunjukkan di bawah ini, dimulai dengan pembuatan ide, perencanaan analisis, dan hasil analisis.



Gambar 1. Bagan Alir Penelitian

2.2. Pengumpulan Data

Melakukan pengamatan secara langsung terhadap objek yang diteliti di Direktorat Sistem Teknologi Informasi (DSTI) Universitas Teknologi Sumbawa sehingga mendapatkan sebuah

informasi terkait dengan topik penulis yaitu protokol keamanan WPA2 dan WPA3 pada jaringan nirkabel. Dan menggunakan studi pustaka Dengan membaca buku, jurnal, artikel, atau dokumen lain yang relevan dengan penelitian yang akan diselesaikan.

2.3. Penetration Testing

a. *Information Gathering* (Pengumpulan Data)

Information Gathering atau Pengumpulan data merupakan kunci utama untuk pengujian. Pada penelitian ini information gathering di lakukan untuk mengumpulkan informasi dari jaringan *wireless* di lokasi penelitian. Data yang dikumpulkan bisa informasi SSID, Enkripsi, dan *MAC Address*.

b. *Vulnerability Detection* (Kerentanan)

Setelah data dikumpulkan, kemudian melakukan deteksi kerentanan dengan tujuan mengetahui celah keamanan dari WPA2 dan WPA3 untuk melakukan uji coba serangan dari informasi yang didapat pada tahap sebelumnya.

c. *Exploit* (Pengujian)

Pengujian dilakukan menggunakan *dictionary attack* menggunakan *tools-tools* pada sistem operasi Kali Linux seperti *airmon-ng, airodump-ng, aireplay-ng,* dan *aircrack-ng*. Serta menggunakan *wireshark* untuk memantau lalu lintas jaringan. Pengujian ini akan menyerang transmisi enkripsi masing – masing keamanan jaringan dalam kondisi online baik itu keamanan WPA2 maupun WPA3. Transmisi yang berhasil direkan akan dideskripsikan untuk mengetahui celah keamanan sebagai tolak ukur perbandingan keamanan yang akan diuji.

Perangkat yang menjadi *access point (smartphone)* akan diubah keamanan jaringannya secara bergantian, setalah satu jenis keamanan telah selesai diuji dengan tahapan yang sama agar dapat mengetahui pada titik pengujian mana yang menunjukkan adanya perbedaan sehingga dapat dijadikan data hasil untuk dianalisis hasil pengujian.

Smarthphone pengguna yang terhubung ke hotspot melalui keamanan WPA2 dan WPA3 menjadi target Dictionary Attack, yang dilakukan oleh penyerang menggunakan sistem operasi Kali Linux yang terinstal di VirtualBox. Untuk memecahkan kata sandi yang digunakan pada enkripsi, tahapan ini memerlukan beberapa serangan yaitu :

1. *Deauthentication Attack*

   Klien yang terhubung akan mengalami kegagalan dan terputus akibat serangan ini, yang akan langsung menyebabkan Penolakan Layanan *(Denial of Service).*

2. *Handshake Capture Dictionary Attack*

   Setelah serangan yang disebutkan sebelumnya, penangkapan *handsake* akan diamati menggunakan *Wireshark*, yang memungkinkan kita mengamati autentikasi enkripsi dan *deautentikasi.*

3. *Cracking Dictionary Attack*

   Serangan ini dilakukan untuk memecahkan kata sandi yang telah didapat pada proses *capture* dengan memanfaatkan *tools aircracking.*

d. *Reporting* (Laporan)

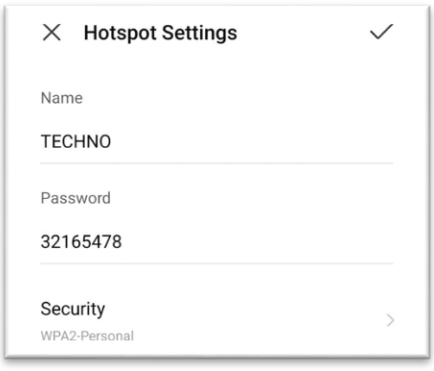
Setelah penetrasi dilakukan, kemudian menyiapkan laporan akhir yang menjelaskan tentang pengujian dan celah keamanan yang telah ditemukan sehingga dapat mengambil tindakan.

3. HASIL DAN PEMBAHASAN

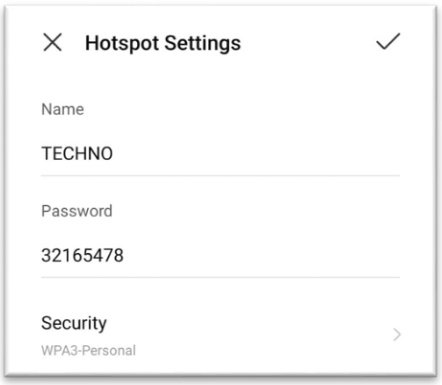
a. *Information Gathering* (Pengumpulan Data)

Information Gathering atau Pengumpulan data merupakan kunci utama untuk pengujian. Pada penelitian ini *information gathering* di lakukan untuk mengumpulkan informasi dari jaringan *wireless.* Data yang dikumpulkan bisa informasi SSID, Enkripsi, dan MAC *Address.*

Pada tahap ini alat yang perlu kita perlukan ialah sebuah adapter *wifi* yang mendukung mode monitor, pada penelitian ini penulis menggunakan USB Adapter TP-LINK TL-WN272 versi 1 dengan *chipset* ATHEROS AR9271. Kemudian mengatur setup *Accsess Point.*



Gambar 2 *Setup WPA2 Personal*



Gambar 3 *Setup WPA3 Personal*

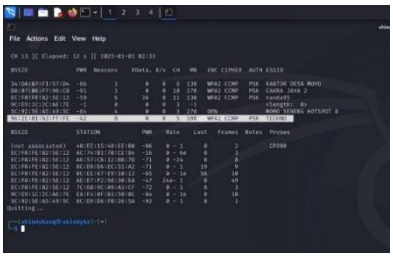
Sebelum melakukan proses pada kali linux penulis mengukur packet loss dan throughput dari protokol keamanan masing masing keamanan. Berikut hasil pengukurannya :

TABEL I. PERBANDINGAN *PACKET LOSS* DAN *THROUGPUT* WPA2 DAN WPA3

Protokol Keamanan	Jumlah Klien	Packet Loss	Rat-Rata Throughput (Kbps)	Rata-Rata Delay (ms)	Rata-Rata Jitter
WPA2-PSK	1	5 (0,018 %)	358K	20,956223	-20,95271
WPA2-PSK	2	10 (0,027 %)	452K	15,680631	0,0002895
WPA2-PSK	4	-	5731	383,89951	0,0061584
WPA2-PSK	10	31 (0,061 %)	537K	11,444624	-0,000378
WPA3-SAE	1	5 (0,017 %)	364K	20,194407	0,0001608
WPA3-SAE	2	9 (0,018 %)	596K	11,890731	-0,000278
WPA3-SAE	4	107 (0,268 %)	398K	14,967001	-0,000206
WPA3-SAE	10	36 (0,062 %)	604K	9,9279082	0,0006774

Tabel di atas menunjukkan bahwa semakin banyakanya perangkat yang terhubung maka jumlah throughput juga semakin tinggi setiap byte per second nya ini menunjukkan bahwa jaringan ini mampu mengirim dan mentransfer data dengan efisien, kecuali pada WPA3 di pengujian 3 karena banyaknya persentase packet loss maka menurun juga jumlah throughput per second ini dikarenakan adanya overhead autentikasi pada WPA3 lebih intensif dibandingkan dengan sebelumnya. Overhead tambahan ini dapat menyebabkan penurunan kinerja jaringan, terutama dalam keadaan banyaknya perangkat yang terhubung secara bersamaan.

Berikutnya kita menjalankan terminal pada Kali Linux dan masuk ke mode monitor agar data seperti MAC *Address*, SSID, dan Enkripsi didapatkan. Selanjutnya kita akan menemukan titik akses dari jaringan dengan menggunakan perintah *sudo airodump-ng wlan0mon*.



Gambar 4 *airodump-ng WPA2* menampilkan titik akses

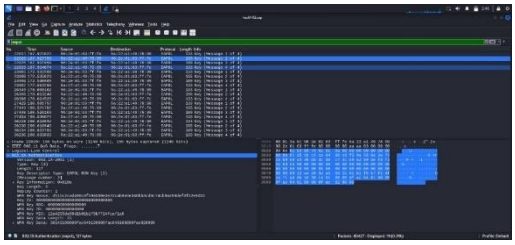
Gambar 5 *airodump-ng WPA3*

Pada gambar 3 di atas bisa dilihat sejumlah jaringan nirkabel telah ditemukan dan bisa dilihat BSSID atau MAC *Address* jaringan nirkabel. Dan jaringan yang penulis gunakan yaitu TECHNO, perhatikan bahwa dia berada di *channel* 5 dengan MAC *Address* 96:2E:01:63:FF:FE dan enkripsi WPA2. Dan pada gambar 4 merupakan informasi mengenai jaringan yang menggunakan enkripsi WPA3 dengan MAC *Address* EE:CC:71:26:17:76 di *channel* 6. Selanjutnya kita akan menggunakan *perintah sudo airodump-ng* wlan0mon -d 96:2E:01:63:FF:FE untuk hanya menampilkan titik akses pada MAC *Address* WPA2 dan perintah *sudo airodump-ng* wlan0mon -d EE:CC:71:26:17:76 untuk menampilkan titik akses jaringan WPA3.

b. *Vulnerability Detection* (Kerentanan)

Setelah data dikumpulkan, kemudian melakukan deteksi kerentanan dengan tujuan mengetahui celah keamanan dari WPA2 dan WPA3 untuk melakukan uji coba serangan dari

informasi yang didapat pada tahap sebelumnya. Pada tahap ini kita akan menangkap *handsake* pada jaringan yang mana kita akan menggunakan perintah *sudo airodump-ng* -w hack1 -c 5 –bssid 96:2E:01:63:FF:FE wlan0mon yang mana hack1 merupakan nama *file* tempat penyimpanan hasil *capture* agar mudah diakses pada *wireshark*, -c 5 merupakan *channel* dari jaringan dan 96:2E:01:63:FF:FE merupakan MAC Address jaringan WPA2. Dan wlan0mon adalah *interfac*e yang kita gunakan. Kita juga menggunakan perintah yang sama untuk jaringan WPA3 yaitu *sudo airodump-ng* -w hack1 -c 6 –*bssid* EE:CC:71:26:17:76 wlan0mon.



Gambar 6 *File* tangkapan WPA2 di *wireshark*

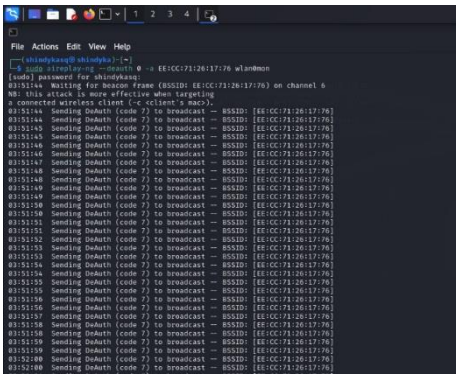
Pada gambar 6 telah menangkap beberapa aktifitas yang telah dilakukan pada jaringan yang menggunakan protokol WPA2. Pada *wireshark* kita mencari *EAPOL (Extensible Authentication Protocol Over LAN).* EAPOL biasa digunakan untuk menjalankan proses autentikasi. Pada EAPOL ini dapat dilihat banyaknya pesan yang dikirim. Perhatikan pada pesan kedua kita dapat melihat data kunci yang dikirim dari perangkat *client* ke perangkat *Access Point* yang selanjutnya data-data tersebut yang dideskripsikan nantinya. Sedangkan untuk protokol WPA3 tidak ada aktivitas yang ditangkap ini dikarenakan pada proses tangkap *handsake* protokol WPA3 tidak dapat menangkap *handsake* sehingga *wireshake* tidak menangkap aktifitas.

c. *Exploit* (Pengujian)

Pengujian dilakukan menggunakan *dictionary attack*, pengujian ini akan menyerang transmisi enkripsi masing – masing keamanan jaringan dalam kondisi online baik itu keamanan WPA2 maupun WPA3. Pada *Dictionary Attack* dimana skenario *attacker* yang menggunakan OS Kali Linux yang *terinstall* pada *VirtualBox* dengan target *smartphone user* yang terhubung ke *hotspot* yang menggunakan keamanan WPA2 dan WPA3. Untuk memecahkan kata sandi yang digunakan pada enkripsi, tahapan ini memerlukan beberapa serangan yaitu :

1. *Deauthentication Attack*

Pada proses ini kita menggunakan perintah sudo aireplay-ng –deauth 0 -a 96:2E:01:63:FF:FE wlan0mon untuk enkripsi WPA2 dan sudo aireplay-ng –deauth 0 -a EE:CC:71:26:17:76 wlan0mon untuk enkripsi WPA3.

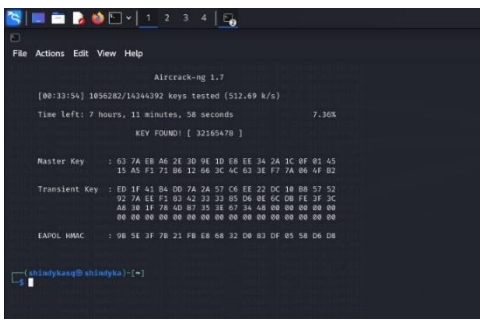


Gambar 7 *Deauthentication* WPA2

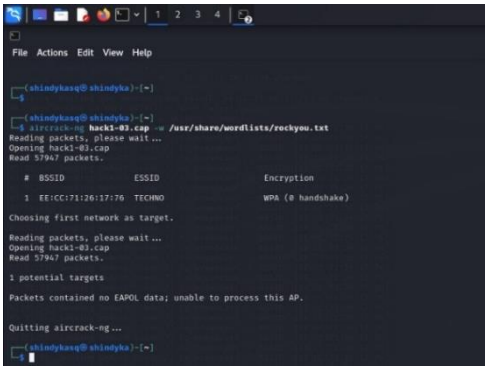
Pada gambar 7 melakukan proses *deauthentication* memutuskan koneksi jaringan pada client dan setelah proses selesaikan serangan *deauthentication* berhasil ketika penulis mencoba kembali untuk menyambungkan jaringan tersebut ternyata tidak berhasil. Sedangkan pada enkripsi WPA3 *deauthentication* tidak berhasil dilakukan sehingga menyebabkan tidak adanya *handsake* yang ditangkap.

2. *Cracking Dictionary Attack*

Serangan ini dilakukan untuk memecahkan kata sandi yang telah didapat pada proses *capture* dengan memanfaatkan *tools aircracking.* Sebelum memulai tahapan ini kita perlu menghentikan mode monitor terlebih dahulu dengan perintah *sudo airmon-ng* stop wlan0mon. Setelah mode monitor dihentikan kita bisa memulai *aircracking* dengan perintah *aircrack-ng hack-02.cap -w /usr/share/wordlist/rockyou.txt.*



Gambar 8 *aircracking* WPA2



Gambar 9 *aircracking* WPA3

Gambar 8 menunjukkan proses dari *aircrak-ng* dari data yang telah didapat pada proses *handsake* sebelumnya untuk memecahkan kata sandi yang ada pada enkripsi WPA2. Pada gambar tersebut menunjukkan bahwa proses tersebut berhasil memecahkan kata sandi enkripsi tersebut yaitu 32165478. Sedangkan gambar 9 menunjukkan *aircrack-ng* untuk WPA3, pada proses tersebut menunjukkan bahwa proses tersebut tidak berhasil dikarenakan tidak ada data yang ditangkap pada proses *handsake.*

d. *Reporting*

Berdasarkan hasil uji enkripsi yang telah dilakukan terlihat bahwa adanya perbedaan pada protokol keamanan, berikut beberapa variabel yang bisa dijadikan perbandingan kedua protokol keamanan yang diujikan dengan melakukan pengujian yang sama. Dari pengujian di atas didapatkan beberapa hasil data seperti berikut :

TABEL II HASIL UJI ENKRIPSI

No	Jenis Serangan	Informasi yang dibutuhkan	Status	
			WPA2	WPA3
1	*Capture Traffic AP*	BSSID, Enkripsi, Channel, dan ESSID	Berhasil	Berhasil
2	*Deauthentication*	*Disconnect* secara paksa	Berhasil	Tidak Berhasil
3	*Capture Handsake*	*Auth system*	Berhasil	Tidak Berhasil
4	*Cracking Dictionary Attack*	Kata Sandi dari Enkripsi	Berhasil	Tidak Berhasil

Deauthentication MAC *Address AP* terhadap *user* berhasil dilakukan pada protokol keamanan WPA2, sedangkan pada WPA3 sebaliknya, sehingga untuk tahap *captured handshake* hingga *aircracking* tidak mungkin dilakukan pada WPA3. Hal ini dikarenakan autentikasi WPA3 menggunakan *Simultaneous Authentication of Equals* (SAE) yang memiliki kelebihan menggunakan algoritma *Password-Authenticated Key Exchange* (PAKE) yang dapat melindungi kata sandi dari pihak ketiga yang tidak berwewenang dan SAE yang menggantikan metode PSK yang menawarkan kunci keamanan yang lebih aman. Sedangkan WPA2 menggunakan autentikasi PSK untuk jaringan personal yang di mana sangat rentan dengan serangan *dictionary* dan tidak adanya perlindungan terhadap kata sandi apalagi kata sandi yang lemah.

4. KESIMPULAN DAN SARAN

Dari hasil pengujian yang telah dilakukan dapat disimpulkan bahwa :

a. Pengumpulan informasi seperti BSSID, enkripsi, *channel*, dan ESSID dapat dilakukan pada jaringan WPA2 maupun WPA3 dengan status berhasil.
b. Serangan *deauthentication* berhasil dilakukan pada jaringan WPA2, tetapi tidak berhasil pada jaringan WPA3. Sehingga untuk tahap *Capture Handshake* sampai *aircracking* tidak akan berhasil dilakukan.
c. WPA3 memiliki perlindungan lebih baik terhadap serangan *dictionary attack*.
d. WPA3 menunjukkan ketahanan lebih baik terhadap sebagian besar serangan, terutama *handshake* dan perlindungan terhadap *cracking password*, sehingga menjadikan WPA3 pilihan yang lebih aman untuk jaringan nirkabel. Namun, pengumpulan informasi *(capture traffic)* masih memungkinkan pada WPA2 dan WPA3, yang membuktikan bahwa perlunya langkah tambahan untuk meningkatkan privasi data.
e. *Penetratio Testing* metode yang efektif untuk mengevaluasi keamanan jjaringan dikarenakan metode ini dapat menilai kerentanan dan celah kemanan sehingga administrator jaringan dapat mengambil langkah-langkah peningkatan keamanan berdasarkan kerentanan yang terdeteksi.

Berdasarkan hasil uji dan kesimpulan penelitian ini, penulis memberikan beberapa saran :

a. Menyembunyikan nama jaringan atau *Extended Service Set Identifier* (ESSID) agar tidak mudah terdeteksi oleh perangkat lain.
b. Melakukan pengawasan terhadap jaringan
c. Ganti kata sandi secara berkala untuk mencegah serangan jangka panjang.

d. Gunakan kata sandi dengan kombinasi huruf, angka, dan simbol.
e. Beralih menggunakan WPA3 jika perangkat *router* dan *client* mendukung.
f. Untuk penelitian selanjutnya agar dapat mengembangkan metode serangan baru untuk mengevaluasi sejauh mana WPA3 dapat bertahan dan membandingkan ketahanan WPA3 dengan protokol yang lain.

5. UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada dosen pembimbing dan rekan-rekan program studi informatika atas dukungan dan masukan selama penelitian ini dilakukan.

Daftar Pustaka:

[1] N. Hayaty, "Buku Ajar: Sistem Keamanan," pp. 1–99, 2020.

[2] J. Doherty, *Wireless and Mobile Device Security*. Jones & Bartlett Learning, 2021. [Online]. Available: https://books.google.co.id/books?id=H30WEAAAQBAJ

[3] R. Rahman *et al.*, *Buku Ajar Keamanan Jaringan Komputer*. PT. Sonpedia Publishing Indonesia, 2024. [Online]. Available: https://books.google.co.id/books?id=fxUFEQAAQBAJ

[4] H. Haeruddin and A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)," *Comb. Manag. …*, vol. 1, no. 1, pp. 508–515, 2021, [Online]. Available: https://journal.uib.ac.id/index.php/combines/article/view/4475

[5] Rindi Insan Cahyadi1, Edhy Sutanta, and Joko Triyono, "Analisis Sistem Keamanan Wpa2 Pada Jaringan Wireless Menggunakan Metode Signal Scanning Dan Mac Changer (Studi Kasus Di Kos Putra Rahma)," *J. Jarkom*, vol. 12, no. 01, pp. 15–25, 2024, doi: 10.34151/jarkom.v12i01.4799.

[6] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, 2014. [Online]. Available: https://books.google.co.id/books?id=DUMyDwAAQBAJ

[7] A. M. C. College, *VM Virtual Box: Virtualization*. Advanced Micro Systems Sdn Bhd. [Online]. Available: https://books.google.co.id/books?id=5NiFDwAAQBAJ

[8] R. W. Beggs, *Mastering Kali Linux for Advanced Penetration Testing*. in Community experience distilled. Packt Publishing, 2014. [Online]. Available: https://books.google.co.id/books?id=nSXiAwAAQBAJ

[9] Sarah Astia Ningsih, Subardin, and Gunawan, "Analisis Kinerja Jaringan Wireless Lan Menggunakan Metode Qos Dan Rma," *AnoaTIK J. Teknol. Inf. dan Komput.*, vol. 1, no. 1, 2023, doi: 10.33772/anoatik.v1i1.5.

[10] D. Ahmad Nur Soleh and A. Tri Arsanto S.Kom, "Analisa Qos (Quality of Service) Menggunakan Simple Queue Dan Queue Tree Menggunakan Mikrotik," *Explor. It*, vol. 11, no. 2, pp. 38–44, 2019, [Online]. Available: http://jurnal.yudharta.ac.id/v2/index.php/EXPLORE-IT/

[11] M. Michael, I. Ruslianto, and R. Hidayati, "Analisis Perbandingan Sistem Keamanan Jaringan Wi-Fi Protected Access 2-Pre Shared Key (WPA2-PSK) Dan Captive Portal Pada Jaringan Publik Wireless," *Coding J. Komput. dan Apl.*, vol. 9, no. 01, p. 108, 2021, doi: 10.26418/coding.v9i01.45902.

[12] D. Erisma Faishol, T. Adi Cahyanto, and M. Rahman, "Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing," *J. Ris. Sist. Inf. Dan Tek. Inform. (JURASIK*, vol. 9, no. 1, pp. 420–432, 2024, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[13] A. B. Nuhaenibudi As-sajid and R. E. Putra, "Analisis dan Pengujian Dictionary Attack terhadap WPA3 Berbasis Script," *J. Informatics Comput. Sci.*, vol. 5, no. 02, pp. 216–222, 2023, doi: 10.26740/jinacs.v5n02.p216-222.

[14] J. W. Creswell and V. L. P. Clark, *Designing and Conducting Mixed Methods Research*. SAGE Publications, 2011. [Online]. Available: https://books.google.co.id/books?id=6tYNo0UpEqkC

[15] M. A. Zakariah, V. Afriani, and K. H. M. Zakariah, *METODOLOGI PENELITIAN KUALITATIF, KUANTITATIF, ACTION RESEARCH, RESEARCH AND DEVELOPMENT (R n D).* Yayasan Pondok Pesantren Al Mawaddah Warrahmah Kolaka, 2020. [Online]. Available: https://books.google.co.id/books?id=k8j4DwAAQBAJ

[16] I. M. L. M. Jaya, *Metode Penelitian Kuantitatif dan Kualitatif: Teori, Penerapan, dan Riset Nyata*. in Anak Hebat Indonesia. Anak Hebat Indonesia, 2020. [Online]. Available: https://books.google.co.id/books?id=yz8KEAAAQBAJ

[17] M. M. Ir. Syofian Siregar, *Metode Pemilihan Kuantitatif: Dilengkapi dengan Perbandingan Perhitungan Manual & SPSS*. Kencana, 2017. [Online]. Available: https://books.google.co.id/books?id=IjTMDwAAQBAJ