Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing

Dimas Erisma Faishol[1], Triawan Adi Cahyanto[2], Miftahur Rahman[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember, Indonesia
Email: dimaserisma@gmail.com[1], triawanac@unmuhjember.ac.id[2], miftahurrahman@unmuhjember.ac.id[3]

Abstract

Information and communication technology is something that is integral to life in today's era. One of them is a wireless network. This research uses the Penetration Testing method to analyze the wireless technology security system that we often use every day. Analyzing wireless network security is carried out using the Penetration Testing method by carrying out attacks on a simulated network, the operating system used to carry out testing is Kali Linux. The results of this research show that network security using the WPA3 protocol is still vulnerable to gaps that can be exploited. This hacking test is only for educational purposes, it is not permitted to commit crimes such as stealing personal data of network users. By knowing this security gap, it will be an evaluation to provide better security.

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

Abstrak

Teknologi informasi dan komunikasi adalah hal yang terpisahkan dari kehidupan di era sekarang ini. Salah satunya yaitu jaringan nirkabel. Pada penelitian ini menggunakan metode Penetration Testing untuk melakukan analisis terhadap sistem keamanan teknologi wireless yang sering kita gunakan setiap hari. Dalam menganalisa keamanan jaringan wireless dilakukan dengan metode Penetration Testing dengan melakukan serangan terhadap jaringan yang disimulasikan, sistem operasi yang digunakan untuk melakukan pengujian adalah Kali Linux. Hasil dari penelitian ini menunjukkan keamanan jaringan yang menggunakan protokol WPA3 masih memiliki rentan terhadap celah untuk dieksploitasi. Uji coba peretasan ini hanya bertujuan sebagai edukasi semata, tidak diperkenankan untuk melakukan tindak kejahatan seperti mencuri data pribadi pengguna jaringan. Dengan mengetahui celah keamanan ini maka akan menjadi salah satu evaluasi agar dapat memberikan keamanan yang lebih baik.

Kata kunci*: WPA3, keamanan jaringan, pengujian penetrasi, analisis, jaringan nirkabel*

1. PENDAHULUAN

Penggunaan teknologi nirkabel meningkat pesat di era saat ini dan digunakan pada berbagai bidang untuk mengirim dan menerima data tanpa koneksi kabel fisik. Namun, kemajuan teknologi ini juga memiliki kekurangan yaitu risiko kerentanan baik dari sisi perangkat maupun sistem[1]. Di sisi lain, masyarakat masih belum paham tentang kerentanan yang ada pada jaringan komunikasi baik melalui jaringan lokal maupun publik. Keamanan jaringan nirkabel merupakan isu penting dalam lingkungan komunikasi data saat ini. Jaringan nirkabel (Wi-Fi) adalah bagian penting dari infrastruktur komunikasi modern yang digunakan di rumah, bisnis, lembaga pendidikan, dan tempat umum lainnya[1] [2]. Oleh karena itu, menjaga keamanan jaringan nirkabel sangatlah penting.

Salah satu protokol keamanan yang umum digunakan dalam jaringan nirkabel adalah WPA3 (*Wi-Fi Protected Access 3*). WPA3 merupakan evolusi dari protokol keamanan WPA2 yang memiliki tingkat keamanan lebih rendah. WPA3 dirancang untuk memberikan tingkat keamanan yang lebih tinggi dibandingkan protokol WPA2 [4][5]. Namun, tidak ada protokol keamanan yang sempurna dan celah kerentanan akan selalu muncul.

Peretasan keamanan komunikasi yang ilegal lebih banyak dilakukan melalui jaringan nirkabel, karena pada jaringan nirkabel memiliki kerentananan yang dapat di eksploitasi daripada jaringan kabel [3][6]. Oleh karena itu, melakukan uji penetrasi keamanan jaringan nirkabel melalui protokol WPA3 dilakukan untuk menemukan celah kerentanan sehingga mencegah penyerangan yang dapat dilakukan oleh *hacker*.

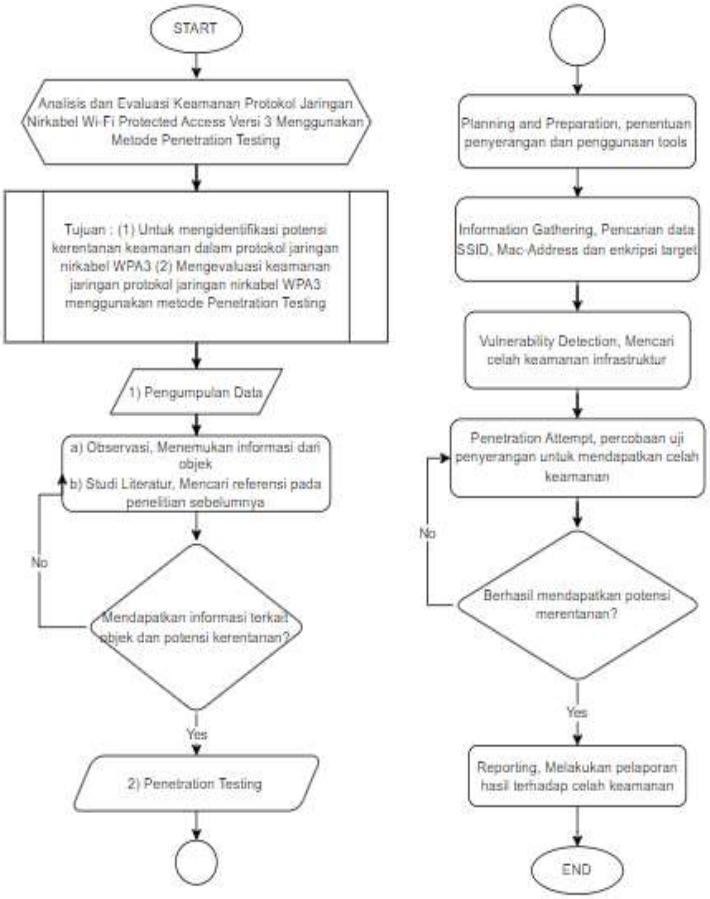
Penetration testing adalah salah satu metode yang efektif untuk mengevaluasi keamanan jaringan dengan menggunakan serangan dari sudut yang berbeda untuk mengeksploitasi kerentanan [7][8]. Sehingga dapat membantu mengidentifikasi potensi kerentanan yang ada pada protokol jaringan nirkabel WPA3.

Pada penelitian sebelumnya [9] dengan judul "A Chosen Random Value Attack on WPA3 SAE Authentication Protocol" peneliti melakukan pengujian serangan menggunakan nilai acak yang dipilih dan serangan perluasannya dengan menghitung kamus nilai acak yang dimasukkan, ditemukan kerentanan pada serangan kamus yang memperoleh informasi tentang sandi dengan menebak kesetaraan skalar, Pada [10] yang berjudul "Analisis dan Pengujian Dictionary Attack Terhadap WPA3 Berbasis Script" peneliti melakukan pengujian menggunakan teknik serangan kamus pada protokol WPA3 dengan kumpulan skrip. [11] melakukan penelitian dengan judul "WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique" peneliti melakukan pengujian *cracking* dengan menggunakan aircrack-ng pada protokol WPA3 dengan melakukan penurunan versi protokol keamanan, sehingga didapatkan hasil pemecahan kata sandi mengunakan aircrack-ng.

2. METODOLOGI PENELITIAN

Metode yang akan digunakan dalam penelitian ini yaitu penetration Testing, yang dimana penetration testing dapat berguna untuk menganalisa seberapa baik sebuah sistem yang ada dapat menangani serangan yang ada. Pentest juga berguna untuk mendeteksi serta merespon adanya penyerangan dengan cepat[12]. Sehingga memiliki tujuan untuk menganalisa risiko yang timbul untuk memberikan rekomendasi pencegahan yang dapat dilakukan ketika sistem yang diuji dapat lolos dari serangan cyber. Adapun tahapan penelitian sebagai berikut[13]:

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 1. Tahapan Penelitian

2.1. Pengumpulan Data

Pada tahap ini peneliti melakukan pengumpulan data menggunakan metode:

a) Observasi
Pada tahap observasi peneliti bertujuan untuk melakukan pengamatan mengenai objek secara cermat demi mendapatkan suatu informasi terkait.

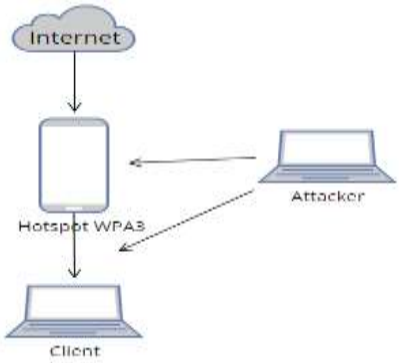
b) Studi Literatur
Setelah mendapatkan informasi dengan melakukan observasi, Selanjutnya peneliti melakukan studi literatur untuk menemukan referensi yang sesuai dengan topik penelitian.

2.2. Penetration Testing

Pada tahap pengujian peneliti menggunakan metode penetration testing dengan tahapan sebagai berikut:

a) Planning and Preparation
Sebelum melakukan tahap awal penelitian, perlu dilakukan planning and preparation untuk menentukan rencana uji coba serangan, topologi, dan alat yang digunakan untuk penelitian ini. Adapun topologi yang digunakan untuk melakukan pengujian adalah:

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

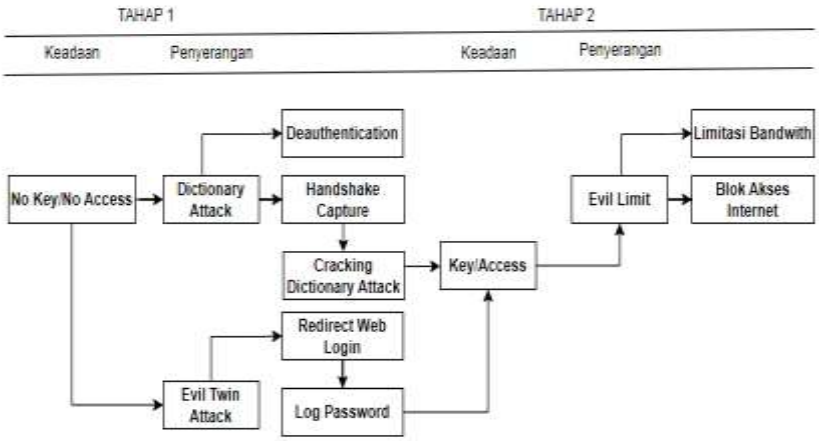


Gambar 2. Topologi

b) Information Gathering
Pada tahap penelitian ini peneliti akan mencari informasi terkait data SSID, Mac-Address, dan Enkripsi.

c) Vulnerability Detection
Tahap deteksi kerentanan bertujuan untuk mencari celah keamanan pada infrastruktur yang sudah ada untuk melakukan uji coba serangan yang telah direncanakan dan diperoleh informasi awal pada tahap *information gathering*.

d) Penetration Attempt
Tahap percobaan pentest dilakukan untuk mendapatkan informasi celah keamanan, serta melakukan uji coba serangan pada infrastruktur yang sudah direncanakan. Adapun Teknik serangan yang direncanakan yaitu:



Gambar 3. Teknik Serangan

e) Dictionary Attack
Pada skenario *attacker* yang menggunakan OS kali linux yang terinstall di virtualbox akan melakukan serangan dengan target laptop user yang terhubung ke hotspot.

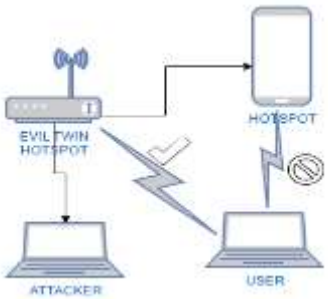
Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Gambar 4. Skenario Dictionary

.

Tahap ini untuk melakukan serangan untuk memecahkan kata sandi yang digunakan pada enkripsi yang digunakan, dengan melakukan beberapa serangan yaitu:

a) Deauthentication Attack
   Serangan ini adalah serangan yang akan langsung menciptakan *Denial Of Service* untuk satu pengguna. Ketika klien yang terhubung akan mengalami kegagalan dikarenakan serangan ini akan mengekploitasi dan kemudian memutus koneksi satu sama lain.
b) Handshake Capture Dictionary Attack
   Setelah serangan *deauthentication* maka akan terdapat *capture* handshake yang dapat kita lihat pada alat Wireshark, pada *capture* ini dapat dilihat proses autentikasi dan *deauthentication* pada enkripsi.
c) Cracking dictionary Attack
   Serangan ini dilakukan untuk memecahkan kata sandi yang telah didapatkan dari *capture* handshake, dengan memanfaatkan alat *aircrack-ng*.
d) Evil Twin
   Tahap skenario penyerang akan membuat *access point* yang sama dengan melakukan *deauth* pada jaringan asli sehingga user akan terputus dan akan menghubungkan kembali dengan mengoneksikan pada jaringan tiruan.



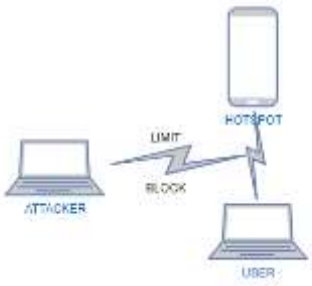
Gambar 5. Skenario Evil Twin

Serangan ini adalah untuk mengelabui klien agar dapat terhubung ke AP asli, namun sebenarnya terhubung ke AP tiruan. Tahap ini dilakukan dengan menggandakan AP asli dengan harapan pengguna akan terhubung kesana. Setelah pengguna terhubung ke AP tiruan penyerang akan dapat melakukan *Man in The Middle Attack* untuk mendekripsi, melihat dan

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

memanipulasi lalu lintas yang diterima dan dikirim pengguna dari perangkatnya.

e) Network Traffic Control
Skenario ini penyerang melakukan ekploitasi komunikasi dengan terhubung dengan jaringan yang sama, sehingga akan dilakukan perubahan *traffic* yang digunakan pada AP yaitu dapat melakukan blok akses internet dan memberi batasan *bandwidth* sehingga pengguna AP tidak bisa menerima paket dengan lancar dan kecepatan yang normal.



Gambar 6. Skenario Evil Limit

f) Reporting
Tahap terakhir yaitu melakukan pelaporan berkaitan tentang pengujian yang telah dilakukan, celah keamanan yang ditemukan. Dengan melampirkan tabel hasil penyerangan.

3. HASIL DAN PEMBAHASAN

Berdasarkan penelitian yang sudah dilakukan, maka diperoleh hasil analisis terkait potensi kerentan pada protokol WPA3 [14]. Dapat dilihat pada Tabel 1.

Tabel 1. Potensi Kerentanan

Serangan	Dipecahkan oleh WPA3
Dictionary Attack	Ya
Evil Twin	Tidak
Krack Exploit	Ya
Deauthentication	Ya
Handshake Capture	Ya

Protokol WPA3 memberikan perlindungan terhadap serangan kamus dan eksploitasi Krack (*Key Reinstallation Attack*) dikarenakan telah memanfaatkan sistem *handshake Simultaneos Authentication of Equals* untuk *forward secrecy* yaitu sebuah fitur keamanan yang mencegah para penyerang dari mendekripsi lalu lintas jaringan yang telah direkam, hal ini mempersulit penyerang untuk membuka *password* Wi-Fi. Namun, serangan Evil Twin belum dapat terpecahkan oleh protokol WPA3 karena serangan ini mencoba mengelabui pengguna agar terhubung dengan AP tersebut dengan mengkloning AP asli dan menawarkan sinyal yang lebih baik dengan harapan klien akan menyambung ke AP tersebut.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

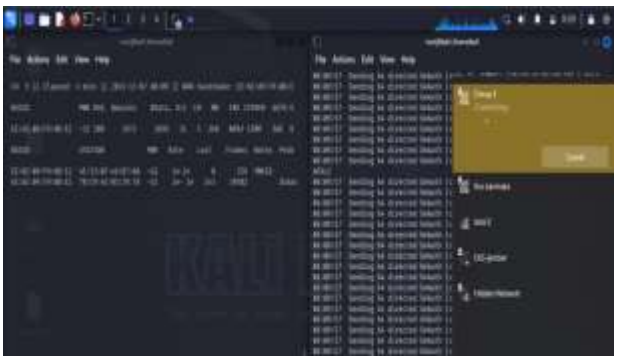
Hasil evaluasi keamanan protokol WPA3 menggunakan metode penetration testing dijelaskan pada tahap sebagai berikut. Tahap yang pertama yaitu masuk ke OS kali linux dengan akses *root* yang telah diinstal pada virtualbox. Tahap selanjutnya yaitu terdapat 3 penyerangan yang akan dilakukan:

3.1. Dictionary Attack

Pada tahap ini akan dilakukan dictionary attack yang dimana tujuan dari serangan ini untuk mengetahui apakah Hotspot yang dilindungi keamanan enkripsi WPA3-Personal dapat mengamankan access pointnya. dengan melakukan beberapa tahapan yang dibutuhkan yaitu Airodump-ng, alat ini digunakan untuk melakukan scanning terhadap Access point yang akan kemudian dilakukan penyerangan melalui informasi BSSID dengan tipe enkripsi WPA3. Dapat dilihat pada Gambar 7.

Gambar 7. Tampilan Airodump-ng

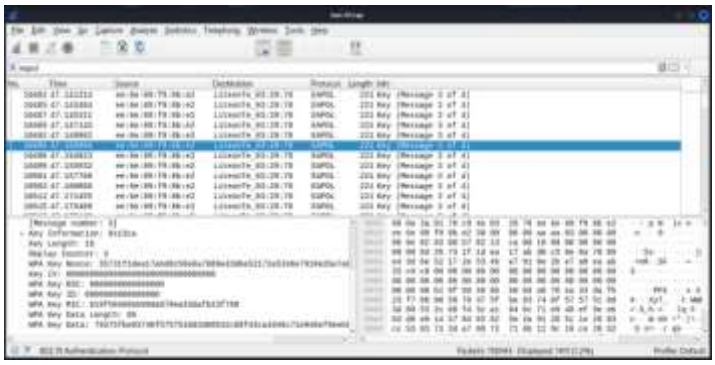
Dari hasil scanning pada Airodump-ng dapat terlihat beberapa jaringan nirkabel sekitar yang berhasil dilakukan scanning sehingga dapat di lakukan penyerangan selanjutnya. Untuk tahap berikutnya yaitu melakukan Deauthentication mengunakan alat aireplay-ng terhadap BSSID (EE:6E:09:F9:08:E2) yang dilindungi keamanan enkripsi WPA3 dengan menargetkan user (70:C9:4E:03:29:78) sebagai pengujian penyerangan, Pada serangan ini harus terdapat user pengguna jaringan tersebut untuk keberhasilan penyerangan sehingga menyebabkan kebocoran rekaman transmisi antara perangkat yang terhubung dengan AP target itu sendiri. Dapat dilihat Gambar 8.



Gambar 8. Hasil Aireplay-ng

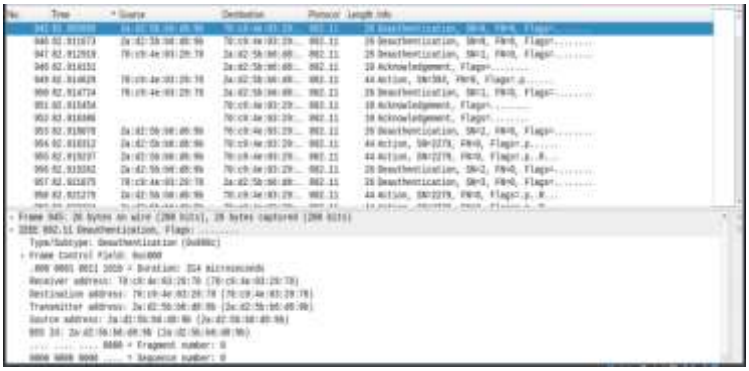
Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Dapat dilihat pada serangan aireplay-ng yang ditargetkan kepada salah satu pengguna hotspot terjadi kebocoran rekaman transmisi data yang menghasilkan capture handshake yang selanjutnya akan dilakukan analisis paket list menggunakan Wireshark sehingga dengan capture packet ini dapat diketahui informasi time, source, destination, protocol, length dan info. Hasil capture packet dapat dilihat pada Gambar 9.



Gambar 9. Hasil Capture Paket

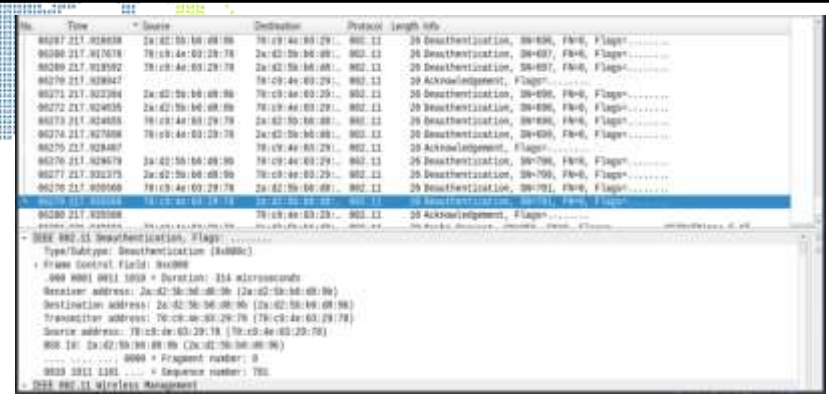
Pada capture packet dapat dilihat juga proses deuthentication yang sebelumnya dilakukan penyerangan. Berikut hasil rekaman waktu transmisi data pada saat dimulainya serangan deauthentication menggunakan aireplay-ng untuk mendapatkan capture handshake menggunakan wireshark.



Gambar 10. Capture start deauth

Dapat dilihat bahwa pada saat proses deauth mengirimkan traffic dalam jumlah yang besar sehingga menyebabkan terputusnya hubungan antar pengguna dengan AP, setelah membanjiri sistem autentikasi maka pengguna akan menghubungkan kembali sehingga akan muncul rekaman autentikasi pada capture handshake. Waktu yang diperlukan dari dimulainya proses deauth yaitu pada time 82 hingga hasil didapatkan dan dihentikannya proses pada time 217 pada Gambar 11 dibawah ini.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 11. Capture end deauth

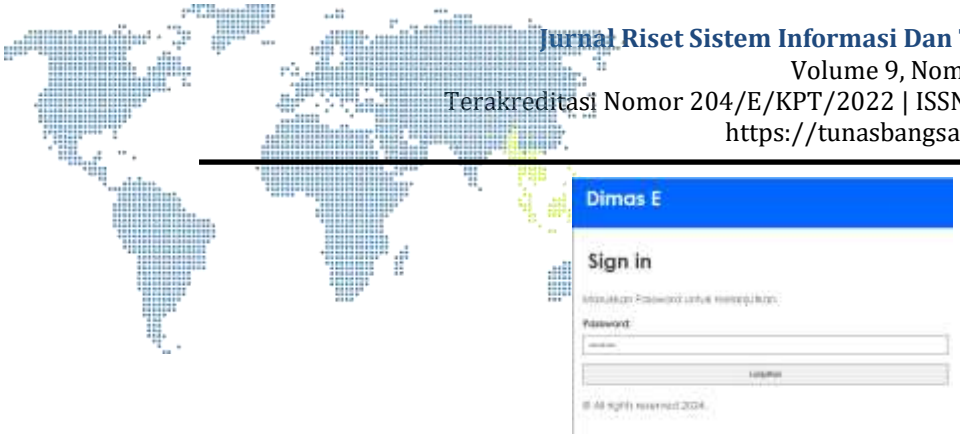
Dengan hasil capture packet yang telah didapatkan pengujian selanjutnya yaitu menggunakan aircrack-ng untuk memecah kata sandi yang digunakan dalam mengamankan jaringan dari hasil capture handshake. Pada percobaan ini berhasil didapatkan kata sandi yang dipakai dikarenakan konfigurasi dan penggunaan password yang tidak beragam maka didapatkan hasil pemecahan kata sandi melalui serangan kamus. dapat dilihat pada Gambar 12.

Gambar 12. Hasil aircrack

3.2. Evil Twin Attack

Pada tahap pengujian ini dilakukan menggunakan alat Evil Twin. Sehingga pengujian ini bertujuan untuk meniru atau menggandakan jaringan wifi asli, tujuannya untuk mengelabuhi pengguna untuk bisa terhubung dengan tiruan AP. Setelah pengguna tertipu dan terhubung ke AP tiruan, protokol WPA3 berada diluar cakupan perlindungannya. Sehingga pengguna akan melakukan auntentikasi password asli dari Access point yang asli dengan SSID “Dimas E”. Dari hasil percobaan ini bisa kita lakukan penggandaan dengan menyebabkan ketika user mencoba terhubung ke Access point tiruan maka akan redirect halaman website untuk memasukkan password yang benar. Dapat dilihat dari hasil Evil Twin pada Gambar 13.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 13. Tampilan redirect evil twin

Dari hasil diatas akan dimasukkan password yang sesuai dengan Access point "Dimas E" maka Evil Twin akan menyelesaikan penggandaannya dengan menghasilkan log password yang telah diinputkan pada halaman website yaitu "0987654321". Dapat dilihat pada Gambar 14.

Gambar 14. Log password

Penyerangan ini bisa didapatkan hasil bukan hanya tentang tipe enkripsi yang digunakan melainkan adanya pengguna yang salah menghubungkan koneksi ke Access point Evil Twin.

3.3. Network Traffic Control

Pada pengujian ini dilakukan untuk memonitoring Access point untuk bisa mengontrol pengguna yang terhubung pada jaringan tersebut. Pengujian ini menggunakan tools Evil Limiter dengan ketentuan penyerang berada didalam jaringan yang sama. Diawali dengan scan pengguna yang terhubung dengan jaringan hotspot.Selanjutnya pada pengujian ini pertama penguji akan melakukan block internet pada pengguna, sehingga pengguna yang terhubung tidak mendapatkan internet pada jaringan tersebut, dapat dilihat pada Gambar 15.

Gambar 15. Blok akses internet

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 420-432
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Dari penyerangan tersebut dihasilkan pada pengguna dengan alamat IP Address 192.168.98.43 tidak mendapatkan akses internet karena penyerang telah mengekploitasi jaringan dengan blok akses internet terhadap pengguna tersebut. Untuk mendapatkan hasil blok internet pengguna akan mencoba akses estudy.unmuh.ac.id dapat dilihat pada Gambar 16.

Gambar 16. Hasil blok internet

Dari hasil diatas pengguna yang terhubung pada hotspot dengan IP Address 192.168.98.43 akan mengalami putus koneksi internet meskipun status terhubung dengan hotspot. Tahap berikutnya yaitu mengeksploitasi jaringan komunikasi dengan melakukan limitasi bandwith pada pengguna hotspot dengan IP Address 192.168.98.43 yang akan dibatasi dengan kecepatan bandwith 4 mb. Tahap ini akan menyebabkan pengguna dengan IP tersebut akan mengalami eksploitasi bandwith yang mengakibatkan akses internet yang kecepatannya dibatasi oleh penyerang.

Gambar 17. Limitasi bandwith

Dari penyerangan tersebut dihasilkan pada pengguna dengan alamat IP Address 192.168.98.43 akan mendapatkan akses internet dengan kecepatan 4 Mb karena telah dilakukan limitasi bandwith oleh penyerang. Untuk mendapatkan hasil limit internet pengguna akan mencoba tes bandwith speedtest.net dapat dilihat pada Gambar 18.

Gambar 18. Hasil Limit

Pada hasil diatas didapatkan kecepatan Download 2.39 Mbps dan Upload 2.84 Mbps, Hal ini diakibatkan oleh adanya eksploitasi komunikasi jaringan dari penyerang dengan melakukan limitasi bandwith dengan maksimal kecepatan 4 Mb.

Dari seluruh tahap pengujian yang telah dilakukan, maka penulis dapat menyampaikan hasil dari dari pengujian keamanan jaringan protokol WPA3 dengan menggunakan metode penetration testing berikut adalah laporan dari hasil pengujian keamanan dapat dilihat pada Tabel 2.

Tabel 2. Hasil Penetration Testing

No.	Jenis Serangan	Informasi yang Dibutuhkan	Status
1.	*Dictionary Attack*	*Dictionary Word*, *Handshake user*, Channel yang digunakan dan BSSID *Access Point*	Berhasil
2.	*Evil Twin*	*BSSID Access Point* target	Memungkinkan
3.	*Traffic Control Network (Evil Limit)*	*BSSID Access Point,* Dalam satu jaringan	Berhasil
4.	*Capture Traffic AP*	*Mac Address, Channel* dan *BSSID*	Berhasil

4. SIMPULAN

Pada penelitian diatas maka dapat disimpulkan pada keamanan protokol jaringan nirkabel menggunakan enkripsi WPA3 masih dapat dilakukan eksploitasi BAHWA potensi kerentanan yang ada pada jaringan nirkabel WPA3, penelitian ini mendapatkan kerentanan pada serangan dictionary attack, evil twin, traffic control, dan handshake capture. Dictionary attack berhasil dengan melakukan serangan deauthetication kolaborasi antara Mac-Adreess AP dan juga station (pengguna) sehingga dapat ditemukan kerentanan untuk menghasilkan handshake, dengan ditemukannya kelemahan pada device pengguna dan juga kata sandi yang tidak beragam maka didapatkan password AP. Serangan Evil Twin berhasil ketika ada pengguna jaringan yang masuk melalui AP tiruan dan memasukkan password asli AP sehingga penyerang mendapatkan password tersebut. Evil Limit berhasil karena mampu melakukan penyerangan pada user pengguna dengan ketentuan penyerang harus berada dalam satu jaringan yang sama.

DAFTAR PUSTAKA

[1] S. E. Prasetyo And R. C. Lee, "Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing," 2021. [Online]. Available: Https://Journal.Uib.Ac.Id/Index.Php/Combines

[2] A. Kurniadi, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Tp-Link Archer A6)," 2021. [Online]. Available: Https://Journal.Uib.Ac.Id/Index.Php/Combines

[3] M. A. Adiguna And B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)," *J. Siskom-Kb (Sistem Komput. Dan Kecerdasan Buatan)*, Vol. 5, No. 2, Pp. 1–8, 2022, Doi: 10.47970/Siskom-Kb.V5i2.268.

[4] E. Lamers, "Securing Home Wi-Fi With Wpa3 Personal," 2021.
[5] B. Indira Reddy And V. Srikanth, "Review On Wireless Security Protocols (Wep, Wpa, Wpa2 & Wpa3)," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, Vol. 5, No. 4, Pp. 28–35, 2019, Doi: 10.32628/Cseit1953127.
[6] R. Rachman *Et Al.*, "Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi," *J. Media Inform. Budidarma*, Vol. 1, No. 1, P. 178, 2021, Doi: 10.30865/Mib.V5i3.2979.
[7] Y. Mulyanto, H. Herfandi, And R. Candra Kirana, "Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi Kasus:Rs H.Lmanambai Abdulkadir)," *J. Inform. Teknol. Dan Sains*, Vol. 4, No. 1, Pp. 26–35, 2022, Doi: 10.51401/Jinteks.V4i1.1528.
[8] H. Haeruddin, "Analisa Dan Implementasi Sistem Keamanan Router Mikrotik Dari Serangan Winbox Exploitation, Brute-Force, Dos," *J. Media Inform. Budidarma*, Vol. 5, No. 3, P. 848, 2021, Doi: 10.30865/Mib.V5i3.2979.
[9] S. Sun And H. T. Canada, "A Chosen Random Value Attack On Wpa3 Sae Authentication," Vol. 3, No. 2, 2022, Doi: 10.1145/3468526.
[10] A. B. N. As-Sajid And R. E. Putra, "Analisis Dan Pengujian Dictionary Attack Terhadap Wpa3 Berbasis Script," Vol. 05, Pp. 216–222, 2023.
[11] E. Baray And N. Kumar Ojha, "Wlan Security Protocols And Wpa3 Security Approach Measurement Through Aircrack-Ng Technique," *Proc. - 5th Int. Conf. Comput. Methodol. Commun. Iccmc 2021*, No. Iccmc, Pp. 23–30, 2021, Doi: 10.1109/Iccmc51019.2021.9418230.
[12] A. A. Putra, "Analisis Dan Evaluasi Keamanan Wireless Lan Pada Pt. Bumi Jage Dalam," *Proceeding Semin. Nas. Ilmu Komput.*, Vol. 1, No. 1, Pp. 138–150, 2021, [Online]. Available: Https://Proceeding.Unived.Ac.Id/Index.Php/Snasikom/Article/View/59
[13] A. Irfansyah, "Langkah-Langkah Penetration Testing Yang Perlu Kamu Ketahui," *Eduparx*, 2023. Https://Eduparx.Id/Blog/Insight/Cyber-Security/Langkah-Langkah-Penetration-Testing-Yang-Perlu-Kamu-Tahu/ (Accessed Jan. 14, 2024).
[14] A. Wi-Fi, C. P. Kohlios, And T. Hayajneh, "A Comprehensive Attack Flow Model And Security," 2018, Doi: 10.3390/Electronics7110284.