RABIT : Jurnal Teknologi dan Sistem Informasi Univrab ISSN CETAK : 2477-2062
Volume 7 No. 1 | Januari 2022 : Hal : 43-51 ISSN ONLINE : 2502-891X

PERBANDINGAN SISTEM AUTENTIKASI WPA2 EAP-PSK PADA JARINGAN WIRELESS DENGAN METODE PENETRATION TESTING MENGGUNAKAN FLUXION TOOLS

[1)] Stefanus Eko Prasetyo, [2)] Try Windranata
[1,2)]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam
[1,2)]Jl. Gajah Mada, Baloi Permai Kec.Sekupang, Kota Batam – Kepulauan Riau - Indonesia
E-mail : [1)]*trywindranata@yahoo.com*, [2)] *stefanus@uib.ac.id*

ABSTRAK
Jaringan Nirkabel merupakan sekumpulan perangkat elektronik yang menghubungkan satu dengan yang lain memanfaatkan perangkat udara alias frekuensi jadi alur lintas data. Masa sekarang ini, ada banyak pengguna yang memanfaatkan WPA2-PSK ataupun WPA2-EAP menjadi *security system* jaringan nirkabel yang bertujuan untuk menghindari orang yang mengakses tanpa izin. Riset ini memakai teknik *wireless penetration testing* yang memakai *fluxion tools* dengan membandingkan dan menganalisis *security system* otentikasi *WPA2* dengan *EAP-PSK* pada jaringan nirkabel yang bertujuan untuk mengetahui kerentanan sebuah sistem keamanan jaringan tersebut. Untuk melaksanakan *penetration testing* penulis mengacu terhadap "*Wireless Network Penetration Testing Methodology*." Yang terdiri dari *intelligence gathering, vulnerability analysis, threat modelling, password cracking,* dan *reporting.* Dari penelitian ini akan menyimpulkan *WPA2-PSK* kurang aman untuk digunakan dikarenakan terlihat pada *penetration testing* tesrsebut *WPA2-PSK* berhasil dibobol dalam keadaan *SSID unhide,* sedangkan *WPA2-EAP* berhasil dalam pembuatan *Web Interface* namun tidak berhasil dalam mendapatkan informasi seperti *username* dan *passwor*. Jika *WPA2-PSK SSID* dalam keadaan *hide* akan mengagalkan peretasan sehingga dari sistem keamanan kedua tersebut memiliki kelebihan dan kekurangan masing-masing tergantung kebutuhan pengguna.

Kata Kunci: *Penetration Testing, Fluxion Tools, WPA2-PSK, WPA2-EAP, Jaringan Wireless*

ABSTRACT
Wireless Network is a collection of electronic devices that connect to each other using air devices or frequencies as a data traffic flow. Today, there are many users who use WPA2-PSK or WPA2-EAP as a wireless network security system that aims to prevent people from accessing it without permission. This research uses a wireless penetration testing technique that uses fluxion tools by comparing and analyzing the WPA2 authentication security system with EAP-PSK on a wireless network which aims to determine the vulnerability of a network security system. To carry out penetration testing, the author refers to the "Wireless Network Penetration Testing Methodology." Which consists of intelligence gathering, vulnerability analysis, threat modeling, password cracking, and reporting. From this study, it will be concluded that WPA2-PSK is less safe to use because it can be seen in the penetration testing that WPA2-PSK was successfully hacked in an unhide SSID state, while WPA2-EAP was successful in making Web Interfaces but failed to obtain information such as usernames and passwords. If the WPA2-PSK SSID is in a hide state, it will fail the hack, so that both security systems have their own advantages and disadvantages depending on the user's needs.

Keyword: *Penetration Testing, Fluxion Tools, WPA2-PSK, WPA2-EAP, Wireless Network*

PENDAHULUAN

Perkembangan teknologi jaringan dari dahulu kala terus berkembang sampai saat ini, adapun jumlah teknologi ditemukan untuk meringankan manusia dalam berkomunikasi. Diantaranya teknologi yang terus berkembang hingga saat ini merupakan teknologi media transmisi jaringan nirkabel [1]. Jaringan Nirkabel merupakan sekumpulan perangkat elektronik yang menghubungkan satu dengan yang lain memanfaatkan perangkat udara alias frekuensi jadi alur lintas data. Pada masa sekarang ini mendirikan jaringan nirkabel cukup mudah. Dikarenakan sejumlah pemasar yang mengadakan kemudahan pada admin

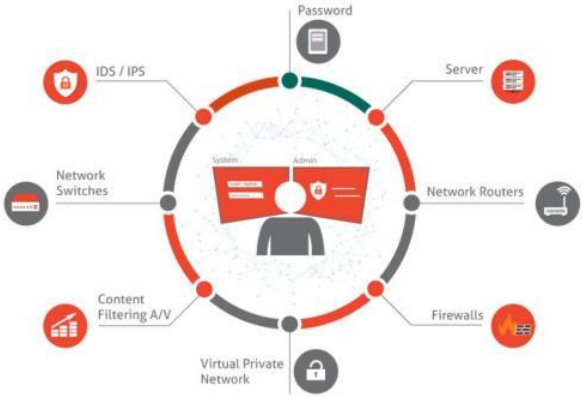
jaringan untuk membuat jaringan nirkabel. Kemudian sewaktu-waktu diketahui jaringan nirkabel yang masih memanfaatkan konfigurasi jaringan bawaan pemasar. Konfigurasi yakni *IP Address*, DHCP *enable*, SSID, *Remote Management*, kanal frekuensi, tanpa enkripsi bahkan *user* atau *password* untuk administrasi jaringan wireless tersebut masih standar bawaan pabrik [2].

Pada umumnya jaringan komputer terdapat beberapa jenis yang berdasarkan area kerja dengan dibedakan menjadi 3 bagian yaitu:

1. *LAN (Local Area Network)* yaitu jaringan komputer yang saling terkoneksi pada 1 area seperti ruangan yang sama maupun gedung yang sama [3].
2. *MAN (Metropolitan Area Network)* merupakan jaringan komputer yang saling terhubung pada satu kota. Jaringan *MAN* menghubungkan *LAN* yang tempatnya berjauhan.
3. *WAN (Wide Area Network)* merupakan jaringan komputer yang saling terhubung pada kota-kota yang berbeda dalam suatu negara dengan menggunakan ISP sehingga komputer bisa berkomunikasi dengan jaraknya yang melintasi sampai antar benua.

Masa sekarang ini, ada banyak pengguna yang memanfaatkan WPA2-PSK menjadi *security system* jaringan nirkabel yang bertujuan sebagai menghindari orang yang tidak mempunyai kewajiban dalam mengakses internet secara illegal [4]. *Authentication* WPA memanfaatkan standar 802.1X serta *Extensible Authentication Protocol* (EAP) [5]. Teknologi jaringan nirkabel yang menggunakan frekuensi tinggi membuatnya rentan terhadap ancaman keamanan. Beberapa aktivitas proteksi mampu dikerjakan dengan menggunakan perangkat komunikasi yang digunakan. Dengan adanya jaringan *wireless*, dapat memberikan sedikit celah keamanan kepada penyerang, misalnya bocornya *password* keamanan WPA2-PSK [6].

Penetration Testing merupakan sub-kategori dalam *Ethical Hacking* yakni salah metode serta langkah yang berfungsi dalam memeriksa ataupun menanungi keamanan informasi. *Penetration Testing* adalah kegiatan menilai *security system* yang telah dibikin dengan menggunakan tiruan serangan yang seringkali dimanfaatkan bagi peretas. Aktivitas tersebut perlu disetujui oleh pemilik sistem. Gambar 1 ini adalah jangkauan *penetration testing* pada alur jaringan komputer yakni *network routers, firewall, server, password, content filtering, VPN, IDS* serta *Network Switch* [7], [8].



Gambar 1. Penetration Testing Dalam Jaringan

Kali Linux merupakan sebuah pembagian dari *Linux* tahap dalam untuk audit keamanan serta *penetration testing*. *Kali Linux* adalah penyusunan ulang dari *Back Track Linux* secara komplet, menuruti tanpa syarat terhadap standar pengembangan Debian [9]. Karakteristik *Kali Linux* yakni:

1) Lebih dari 300 *tools penetration testing.*
2) Dapat digunakan secara gratis
3) Mengikuti FHS *compliant*
4) Dukungan perangkat jaringan nirkabel yang luas
5) Lingkungan pengembangan yang aman
6) Dukungan berbagai Bahasa

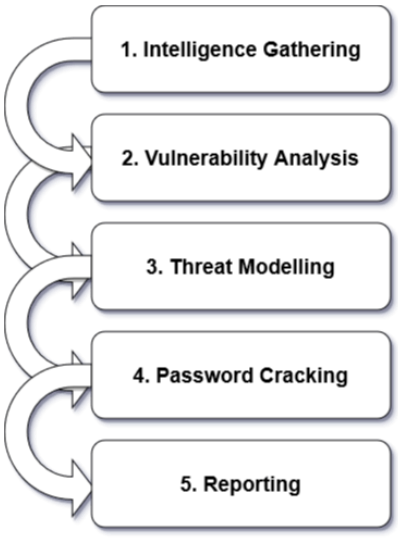
Fluxion merupakan alat audit keamanan dan penelitian rekayasa sosial. *Fluxion tools* yaitu pembuatan Linset oleh vk496 yang memiliki banyak fungsionalitas. *Script* yang digunakan untuk mencoba mengambil *WPA* atau *WPA2 key* dari titik akses target melalui serangan manipulasi psikologis (phising). Pengaturan serangan Fluxion kebanyakan manual, tetapi mode otomatis eksperimental menangani beberapa parameter pengaturan serangan [10].

Masa sekarang ini, ada banyak pengguna yang memanfaatkan WPA2-PSK menjadi *security system* jaringan nirkabel yang bertujuan sebagai menghindari orang yang tidak mempunyai kewajiban dalam mengakses internet secara illegal. Berdasarkan permasalahan tersebut, riset ini memakai teknik *wireless penetration testing* yang memakai *fluxion tools* buat membandingkan dan menganalisis *security system* otentikasi *WPA2* dan *EAP-PSK* pada jaringan nirkabel.

METODE

Untuk melaksanakan *penetration testing* penulis mengacu terhadap "*Wireless Network Penetration Testing Methodology*." Dibawah ini penulis jelaskan teknik *penetration testing* yang berarti yaitu:

1. Intelligence Gathering
   Langkah ini ialah langkah mengumpulkan informasi mengenai jaringan dan layanan aplikasi, menemukan informasi mengenai objek yang diserang atau membuat jejak pada durasi yang telah ditentukan. Sepanjang langkah ini, penguji mencoba mendapatkan informasi pada perangkat *wireless* dengan menggunakan metode *Wireless-Analyze* yang ada pada *fluxion tools* sehingga informasi bisa berupa *SSID, Channel*, Standar *Wireless, MAC Address*, Metode Autentikasi (WEP, WPA, WPA2)
2. Vulnerability Analysis
   Langkah ini penulis akan menelusuri dan memutuskan kualitas keamanan, dan menganalisis layanan yang diberikan, *program* serta versi dari aplikasi tersebut untuk mengetahui kualitas keamanan.
3. Threat Modelling
   Informasi yang didapatkan sebelumnya telah mempermudah penguji untuk menganalisa dan menggunakan *FakeAP* Hostapd sebagai serangan yang dimana akan memanipulasi *wireless target*.
4. Password Cracking
   Pada tahapan ini penguji melakukan *handshake* pada *fluxion* tools terhadap *user* yang terkoneksi dalam jaringan *wireless* yang telah di manipulasi sehingga penguji mendapatkan sebuah paket berupa kode enskripsi untuk dipecahkan menjadi *password* sesuai dengan metode yang telah disiapkan dalam tahapan *Threat Modelling*.
5. Reporting
   Reporting yaitu hasil akhir dari pengujian sistem. Penguji medokumentasikan hasil dari penelitian dalam bentuk sebuah laporan.



Gambar 2. Kerangka Kerja Penelitian

HASIL

Penulis akan melakukan *penetration testing* terhadap *WPA2-PSK* dan *WPA2-EAP*. Penulis menggunakan *fluxion tools* dalam *penetration testing* untuk pengujian sistem keamanan *WPA2-PSK* dan *WPA2-EAP*. Berikut adalah penjelasan tahapan *penetration testing*.

Penetration Testing Pada Security WPA2-PSK (SSID Un-Hide)

1. *Login* ke *configuration router* D-LINK untuk mengatur *security mode* dalam *WPA/WPA2-PSK*.

Gambar 3. Configuration WPA2-PSK pada router D-LINK DIR-600L

2. Pada *fluxion tools* akan dilakukan *handshake* terlebih dahulu terhadap *router*.

Gambar 4. Tampilan awal Fluxion Tools pada WPA2-PSK

3. Pilih *router* yang ingin dibuat untuk melakukan *penetration testing*.

Gambar 5. WiFi List yang didapatkan pada WPA2-PSK

4. Setelah terdapat *user* yang terhubung dalam *router* tersebut, disini *aireplay-ng deauthentication* bekerja untuk memutuskan *user* tersebut sehingga dari *user* diperlukan untuk melakukan *connect* ulang terhadap *router*.

Gambar 6. Progres handshake mendapatkan client pada WPA2-PSK

5. Di langkah ini terlihat bahwa *handshake* telah dilakukan secara sukses dan tutup

terminal yang menyatakan sukses tersebut.

Gambar 7. Handshake berhasil pada WPA2-PSK

6. Pilih *captive portal* untuk melakukan *web interface* terhadap *user* yang terhubung dalam *router*.

Gambar 8. Lanjutan serangan Evil Twins pada WPA2-PSK

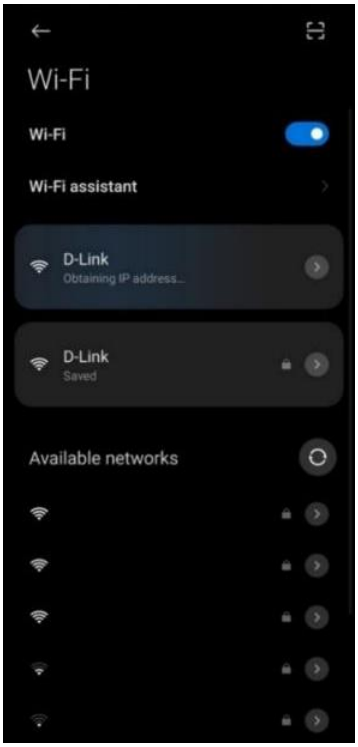
7. Pilih *rogue AP – hostapd* yang bertujuan untuk membuat *pc* ataupun laptop dapat menjadi *access point*.

Gambar 9. Hostapd pada WPA2-PSK

8. Pada langkah ini merupakan tampilan *web interface (evil twin)* yang terdapat *DHCP Services, DNS Services, Web service, Authentication / Wifi Information* serta *Jammer Service.*

Gambar 10. Tampilan Evil Twins pada WPA2-PSK

9. Pada tampilan *user* terdapat *Fake-AP* yang telah dibuat dan telah dialihkan kedalam *web interface*.

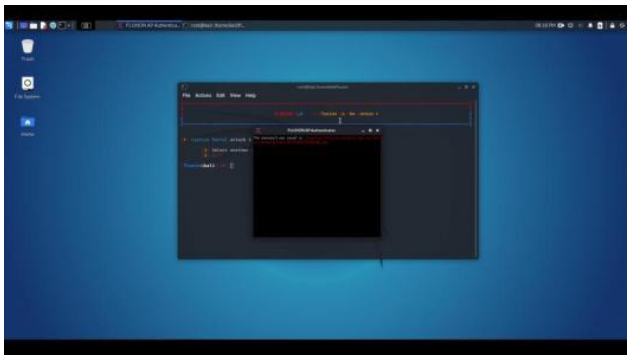


Gambar 11. Tampilan Fake AP pada WPA2-PSK

10. Pada tampilan *user* terhadap berhasil *connect* ke dalam *Fake-AP* yang telah dibuat.

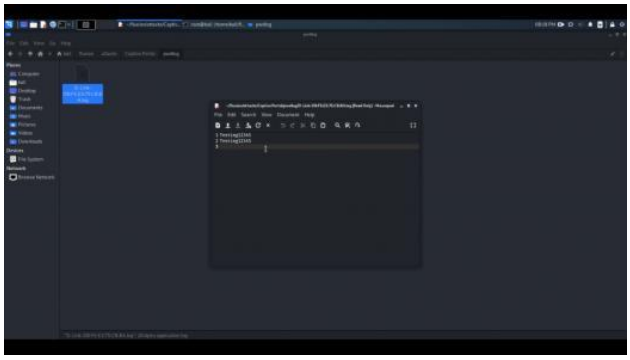
Gambar 12. Tampilan client berhasil connect Fake AP pada WPA2-PSK

11. Jika *user* berhasil *reconnect* terhadap *Fake-AP* maka akan terdapat status *"the password was in ..."*, namun jika gagal *connect* ke dalam *Fake-AP* maka dapat diartikan gagal bobol *wireless* tersebut.



Gambar 13. Tampilan berhasil pada evil twins pada WPA2-PSK

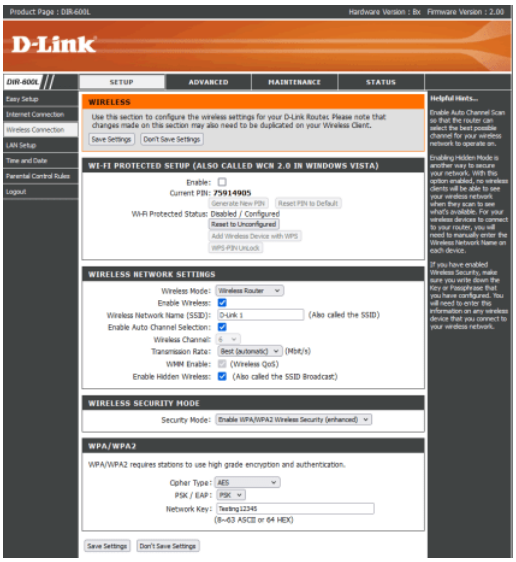
12. Disini terdapat *password* dari *router* tersebut yang menggunakan *security mode* dengan *WPA/WPA2-PSK*



Gambar 14. Password router pada WPA2-PSK

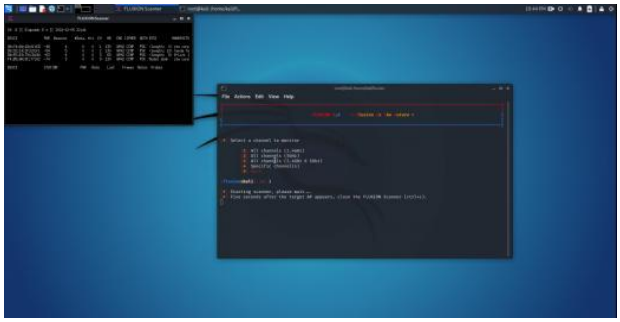
Penetration Testing Pada Security WPA2-PSK (Hide SSID)

1. *Login* ke *configuration router* D-LINK untuk mengatur *security mode* dalam *WPA/WPA2-PSK* dan memastikan *Hidden Wireless* dan *WPS* keadaan non-aktif.



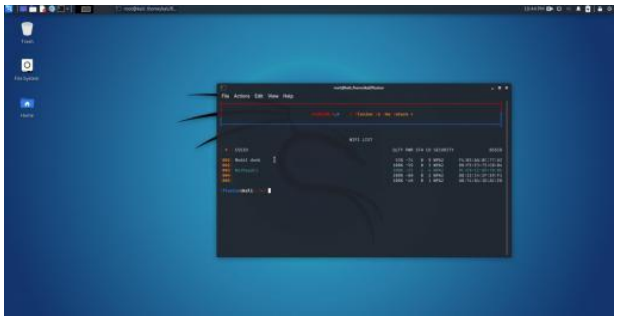
Gambar 15. Configuration WPA2-PSK (Hide SSID) pada router

2. Pada langkah ini, terlihat ada terbaca *SSID* dari *router* tersebut dan penulis mencoba mengingatkan *MAC Address* dari *router* tersebut.



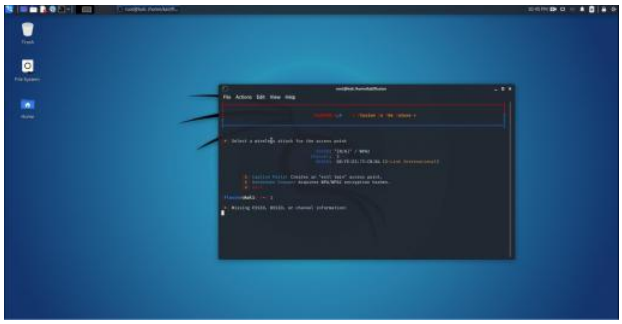
Gambar 16. Scanning WiFi List pada WPA2-PSK (Hide SSID)

3. Terlihat *SSID* tersebut tidak muncul disini, namun penulis mencoba menggunakan *MAC Address* yang telah dicatat tadi.



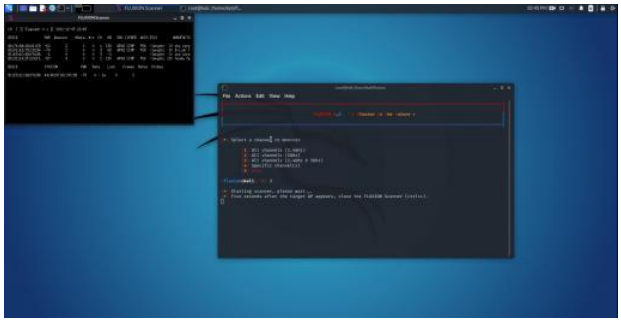
Gambar 17. WiFi List yang didapatkan pada WPA2-PSK (Hide SSID)

4. Setelah berhasil melakukan *handshake*, penulis ingin melanjutkan ke dalam *captive portal* namun terjadi *Missing SSID*.



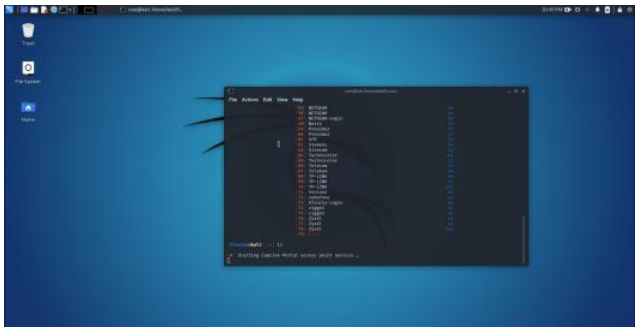
Gambar 18. Lanjutan serangan Evil Twins pada WPA2-PSK (Hide SSID)

5. Disini kita memilih ulang *SSID* yang ingin dilakukan *penetration testing*.



Gambar 19. Memilih ulang WiFi pada WPA2-PSK (Hide SSID).

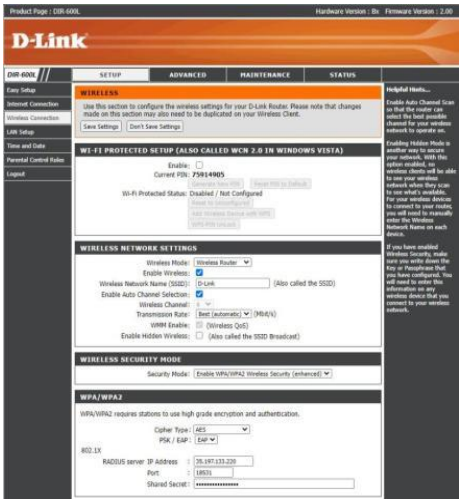
6. Ketika ingin melakukan pembuatan *web interface* namun berhenti pada bagian *starting captive portal* sehingga tidak terbuat *web interfacenya*.



Gambar 20. Gagal Membuat web interface pada WPA2-PSK (Hide SSID)

Penetration Testing Pada Security WPA2-EAP

1. *Login* ke *configuration router* D-LINK untuk mengatur *security mode* dalam *WPA/WPA2-EAP*.

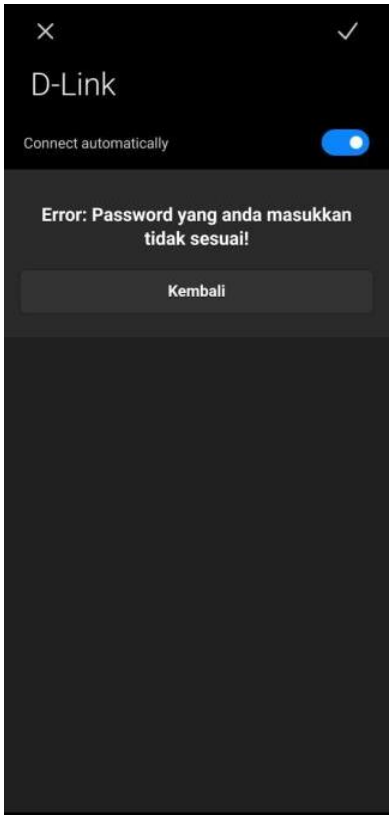


Gambar 21. Configuration WPA2-EAP pada router D-LINK DIR-600L

2. Pada langkah ini terdapat *user* yang mencoba melakukan *reconnect* terhadap *Fake-AP* yang telah dibuatkan.

Gambar 22. Client mencoba connect pada WPA2-EAP

3. Pada tampilan *user* terdapat gagal *connect* terhadap *Fake-AP*.



Gambar 23. Tampilan client gagal connect Fake AP pada WPA2-EAP

Berdasarkan hasil pengujian sebelumnya, penulis memutuskan membuat table perbandingan untuk membandingkan hasil kedua autentikasi sebelumnya. Berikut adalah table pengujian pada penelitian ini.

Jenis Autentikasi	Status	Informasi yang didapatkan
WPA/WPA2 – PSK (SSID Non-Hide)	Berhasil	Pada jenis autentikasi ini berhasil dibobol dengan menggunakan *fluxion tools* dikarenakan tidak membutuhkan *username* dan *password* untuk menghubungkannya
WPA/WPA2 – PSK (SSID Hide)	Gagal	Pada jenis autentikasi ini gagal dibobol karena *SSID* dalam keadaan tersembunyi akan menyulitkan peretas untuk melakaukan pembuatan *web interface*.
WPA/WPA2 - EAP	Gagal	Pada jenis autentikasi ini gagal membobol dikarenakan pada autentikasi *EAP* menggunakan *radius server* yang terdapat *username* dan *password* sedangkan *web interface* pada *fluxion tools* hanya dapat menggunakan *password* untuk menghubungkan.

Tabel 1. Hasil Pengujian

KESIMPULAN

Berdasarkan penelitian yang berjudul "Perbandingan Sistem Keamanan Autentikasi WPA2 dan EAP-PSK Pada Jaringan Wireless Dengan Metode *Penetration Testing* Menggunakan *Fluxion Tools*" maka dapat disimpulkan bahwa *WPA2-PSK* kurang aman untuk digunakan dikarenakan terlihat pada *penetration testing* tersebut *WPA2-PSK* berhasil dibobol dalam keadaan *SSID* aktif, sedangkan *WPA2-EAP* berhasil dalam pembuatan *Web Interface* namun tidak berhasil dalam mendapatkan informasi seperti *username* dan *password*. Jika *SSID WPA2-PSK*

dalam keadaan tersembunyi akan mengagalkan pembobolan bagi peretas. Pada dasarnya *WPA2-PSK* merupakan sistem keamanan jaringan yang paling sering digunakan dalam dunia jaringan dan *WPA2-EAP* merupakan sistem keamanan jaringan yang lebih sedikit penggunanya, dikarenakan *WPA2-EAP* membutuhkan *Radius Server* yang selalu aktif ataupun hidup sebagai *username* dan *password* pada konfigurasi tersebut sedangkan *WPA2-PSK* hanya diperlukan *password* sudah bisa dipakai oleh penggunanya. Sehingga dari sistem keamanan kedua tersebut memiliki kelebihan dan kekurangan masing-masing.

Pada penelitian ini terdapat saran yang ingin disampaikan oleh penulis yaitu menyembunyikan *SSID* jika ingin menggunakan *security mode WPA2-PSK* dan mengkonfigurasi sistem keamanan jaringan sendiri tanpa menggunakan konfigurasi *default*. Dikarenakan jenis serangan pada sistem keamanan jaringan sangat banyak. Ketika mengkonfigurasi sendiri akan mengetahui sistem keamanan yang mana cocok untuk dipakai..

DAFTAR PUSTAKA

[1] E. Rilvani, "Rancang Bangun Jaringan LAN dan Wireless LAN pada SMKN 1 Cikarang Pusat Menggunakan Mikrotik," *J. Teknol. Pelita Bangsa*, vol. 7, no. 2, pp. 179–185, 2017.

[2] D. M. Sari, M. Yamin, and L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) MAC Address, Menggunakan Metode Penetration Testing," *Inf. Secur. Manag. Handbook, Sixth Ed.*, vol. 3, no. 2, pp. 203–208, 2017.

[3] F. Roma Doni, "Jaringan Komputer dengan Router Mikrotik," *Tek. Komput. AMIK BSI*, pp. 88–93, 2016.

[4] E. Wahyudi, "Analisis Keamanan WPA2-PSK Dan Radius Server Pada Jaringan Nirkabel Menggunakan Metode Wireless Penetration Testing," *J. Ilm. Rinjani_Universitas Gunung Rinjani*, vol. 6, no. 1, pp. 199–206, 2018.

[5] E. S. Wati and D. Apriansyah, "Sistem Keamanan Jaringan Wireless Menggunakan Peap Ms Chap," *J. ONESISMIK*, vol. 1, no. 1, pp. 1–9, 2019, [Online]. Available: https://jurnal.dcc.ac.id/index.php/onesismik/article/view/241.

[6] Baihaqi, Y. Yanti, and Zulfan, "Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi," *J. Serambi Eng.*, vol. 3, no. 1, pp. 248–254, 2018.

[7] A. Hidayat and I. P. Saputra, "Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia.Net, Tanjung Harapan Lampung Timur)," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 118–124, 2018, doi: 10.31598/jurnalresistor.v1i2.323.

[8] H. D. Sabdho and M. Ulfa, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang," *Semhavok*, vol. 1, no. 1, pp. 15–24, 2018.

[9] M. I. Rusdi and D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," *Semin. Nas. Teknol. Inf. dan Komput. 2019*, pp. 260–269, 2019.

[10] Cyberfee, L3op, Dlinkproto, Vk496, and MPX4132, "Fluxion," *kali.tools*, 2016. https://en.kali.tools/?p=235.